



D8.1: Standardization Plan

Work Package	8 Standardization and Exploitation
Task	8.1 State of the art for (multimodal) transport standards and Standardization Plan
Authors	Dr. Olga Radchuk Dipl.-Ing. Jörg Nachbaur Alexandra Gapp Dr. Karl Grün
Dissemination Level	PU
Status	Final
Due Date	31/08/2022
Document Date	15/11/2022
Version Number	1.1

Quality Control

	Name	Organisation	Date
Editor	Karl Grün	ASI	27/06/2022
Peer review 1	Fabio Podda Germana Gianquinto	AMT	30/06/2022
Peer review 2	Thierry Henault Yves Brochet Pierre Gauducheau Francois-Xavier Picavet Fabien Joseph	DXT	04/07/2022
Authorised by (Technical Coordinator)	Jason Sioutis	ICCS	21/07/2022
Authorised by	Vasileios Sourlas	ICCS	29/07/2022



This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 883321. Content reflects only the authors' view and European Commission is not responsible for any use that may be made of the information it contains.

(Quality Manager)			
Submitted by (Project Coordinator)	Angelos Amditis	ICCS	31/08/2022

Document Revision History

Version	Date	Modification	Partner
0.1	02.02.2021	First draft	ASI
0.2	01.02.2022	Second draft with further contributions from partners included	ASI
0.3	02.06.2022	Third Draft circulated to project for feedback	ASI
0.4	27.06.2022	Fourth Draft with feedback from partners included	ASI
0.5	05.07.2022	Fifth Draft with comments from peer reviews endorsed	ASI
1.0	21/07/2022	Final review	ICCS
1.1	22/11/2022	Revised Deliverable addressing recommendation 2, i.e. indicating which partners will be active in which standardization organization and what will be the contribution to the respective standard.	ASI

Legal Disclaimer

CitySCAPE is an EU project funded by the Horizon 2020 research and innovation programme under grant agreement No. 883321. The information and views set out in this deliverable are those of the author(s) and do not

necessarily reflect the official opinion of the European Union. The information in this document is provided “as is”, and no guarantee or warranty is given that the information is fit for any specific purpose. Neither the European Union institutions and bodies nor any person acting on their behalf may be held responsible for the use which may be made of the information contained therein. The CitySCAPE Consortium members shall have no liability for damages of any kind including without limitation direct, special, indirect, or consequential damages that may result from the use of these materials subject to any liability which is mandatory due to applicable law.

Table of Contents

List of Figures	6
List of Tables	6
Executive Summary	8
1 INTRODUCTION	9
1.1 Project Introduction	9
1.2 Deliverable Context	9
1.2.1 Objectives of the WP8 Standardization and Exploitation	9
1.2.2 Objectives of the Tasks	10
1.2.3 Deliverable interdependencies	10
1.2.4 Purpose of the Deliverable 8.1	11
1.3 Standardization in a nutshell	11
1.4 Methodology	14
1.4.1 Overview of the standardization landscape	14
1.4.2 Analysis of standardization gaps and needs	14
2 Standardization landscape	15
2.1 Formal standards	15
2.2 Non-formal standards	16
3 Standardization Gaps and needs	17
3.1 Survey results	17
3.2 Standardization focus points for the CitySCAPE consortium	21
4 Standardization Plan	22
4.1 General	22
4.2 Strategic Areas of Participation	23
4.2.1 CEN/TC 278, Intelligent transport system	23
4.2.2 ISO/IEC JTC 1/SC 27, Information security, cybersecurity and privacy protection	25
4.2.3 NIST	28
4.2.4 MobilityData	28
4.2.5 OASIS	29
4.2.6 The MITRE Corporation	29
4.2.7 MANDIANT	30
4.2.8 ENISA	30
4.2.9 Syslog	30
4.2.10 Center for Internet Security (CIS)	30
4.3 Contribution to standardization	31

5	CONCLUSION	33
6	References	34
	ANNEX 1: GAP ANALYSIS SURVEY WITH RESPONSES	35
	ANNEX 2: LIST OF IDENTIFIED FORMAL STANDARDS	44
	ANNEX 3: LIST OF IDENTIFIED NON-FORMAL STANDARDS	197

List of Figures

Figure 1: PDCA methodology for the CitySCAPE standardization plan	22
Figure 2: responses to question 2	36
Figure 3: responses to question 7	40
Figure 4: responses to question 9	41
Figure 5: responses to question 12	43

List of Tables

Table 1: Standardization bodies and number of formal standards.....	16
---	----

List of Abbreviations and Acronyms

Abbreviation	Meaning
CEN	European Committee for Standardization
CENELEC	European Committee for Electrotechnical Standardization
EN	European Standard
ENISA	European Union Agency for Cybersecurity
ETSI	European Telecommunications Standards Institute
ICT	Information and communication technology
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
ISO	International Organization for Standardization
PT	Public Transport
SB	Standardization Body
SDO	Standards Development Organisation
TC	Technical Committee
TR	Technical Report
TS	Technical Specification

Executive Summary

The Standardization Plan provides an overview of the future standardization activities based on the needs of the CitySCAPE project consortium in the area of city transportation to be undertaken during and after the end of the project.

This Plan is drafted by Austrian Standards International (ASI) in collaboration with Institute of Communication and Computer Systems (ICCS), Airbus Cybersecurity SAS (ACS), European Dynamics Luxembourg SA (ED), Kaspersky Lab Italia Srl (KSP), Tallinna Linn (TALLINN), Riigi Infosüsteemi Amet (CERT-EE), CS GROUP (DXT), Azienda Mobilità e Trasporti Spa (AMT), STAM Srl (STAM), Gruppo SIGLA Srl (SIGL), University of Piraeus Research Center (UPRC), OPPIDA (OPP) and Engineering - Ingegneria Informatica Spa (ENG).

It provides an overview of the relevant standards identified during the investigation of the standardization landscape, lists the gaps identified as a result of gap analysis, and summarizes the priority topics to be addressed within the future standardization activities. It covers topics of wide importance for all spheres of public transportation, including ICT infrastructure, personal identification, IoT and electrical equipment. Following a Plan-Do-Check-Act methodology the standardization plan contains focus areas of strategic participation in standardization and a description of actions how and which standards are implemented in the project. In addition, the standardization plan contains the information, which project partners is active in which standardization organization and what will be the contribution to the respective standard and/or the proposal for a new standard.

1 INTRODUCTION

1.1 Project Introduction

The traditional security controls and security assurance arguments are becoming increasingly inefficient in supporting the emerging needs and applications of the interconnecting transport systems, allowing threats and security incidents to disturb all dimensions of transportation.

CitySCAPE is a project funded by the EU's Horizon 2020 research and innovation program, which consists of 15 partners from 6 European countries, united in their vision to cover the cybersecurity needs of the multimodal transportation.

More specifically, the CitySCAPE software toolkit will:

- ✓ Detect suspicious traffic-data values and identify persistent threats
- ✓ Evaluate an attack's impact in both technical and financial terms
- ✓ Combine external knowledge and internally-observed activities to enhance the predictability of zero-day attacks
- ✓ Instantiate a networked overlay to circulate informative notifications to CERT/CSIRT authorities and support their interplay.

The project duration extends from September 2020 to August 2023.

1.2 Deliverable Context

1.2.1 Objectives of the WP8 Standardization and Exploitation

This deliverable is the first out of three within the WP8. The WP8 is focused on a variety of exploitation activities, including standardization and security labelling for public transport to support the future market acceptance and uptake of the project results.

The general objectives of the WP8 are:

1. Elaborate and implement a standardization plan based on the relevant formal and non-formal standards – existing or under development.
2. Develop recommendations for security labelling process for public transport systems.
3. Conduct a market analysis and map the consortium's needs vs. solutions identifying potential value opportunities for exploitation of the project results, as well as their associated market technical benefits and risks.

1.2.2 Objectives of the Tasks

T8.1: State of the art for (multimodal) transport standards and Standardization Plan

The objectives of the task 8.1 are:

1. Identify and provide an overview of the formal and non-formal cybersecurity standards (existing and under development), applicable for Public transport systems.
2. Evaluate the available standards against the needs of the project partners.
3. Elaborate a standardization plan reflecting the partners' needs and update the plan regularly within the duration of the project.

T8.2: Standardization Activities in support of a security labelling for transport

The objectives of the task 8.2 are:

1. Evaluate the feasibility of security labelling for public transport systems.
2. Elaborate recommendations for such security labelling in form of a proposal for a standard that falls within the scope of ISO or CEN in the area of information security, cybersecurity and privacy protection.

T8.3: Market analysis and sustainable exploitation strategies

The objectives of the task 8.3 are:

1. Conduct a market analysis determine the positioning of project results in the current market context.
2. Identify relevant stakeholders, customers and competitors, their main concerns and challenges to adopt the project solutions, as well as the market drivers and barriers.
3. Elaborate a number of business cases cover needs and solutions.
4. Identify potential success areas and gaps to be filled by the project results.
5. Elaborate a report containing the market analysis and value opportunities of the project results.

1.2.3 Deliverable interdependencies

The standardization plan elaborated within the **T8.1** will ensure that the project activities are conducted in line with the opportunities, identified within the **T8.3** and address the relevant stakeholders. In addition, **D8.1** will provide the background for the deliverable **D8.2** Recommendations and options for a security labelling for transport.

Considering the CitySCAPE project as a whole, the standardization plan, developed in the WP8, will serve as a cornerstone for the work, conducted within the

- WP5 CitySCAPE security layer implementation,
- WP6 Data handling and CitySCAPE solution integration and
- WP7 Pilot demonstrators and validation.

Trust into and acceptance of any proposed cybersecurity solution is directly related to its compliance to standards, which guarantees the reliability and interoperability of such a solution.

1.2.4 Purpose of the Deliverable 8.1

The purpose of the D8.1 Standardization Plan is to address the first objective of the WP8 and elaborate and implement a standardization plan, based on the relevant standards (existing or under development), and provide it to the other WPs for further exploitation. This will ensure that project results are aligned with current regulations and on-going standardisation activities.

The Standardization Plan outlines the initial standardization roadmap in the area of cybersecurity in transport system, based on the investigation of the standardization landscape, the standardization gaps identified using an online survey, and on the standardization needs of CitySCAPE consortium partners.

The first version of Standardization Plan constitutes the Milestone 12, due in Month 6 (February 2021).

The second version of the Standardization Plan constitutes the Milestone 19. Next to an update of identified standards listed in the first version, it includes the actions for the focus areas of strategic participation in standardization and a description of actions how and which standards are implemented in the project.

The present version is the result of two feedback cycles having requested CitySCAPE consortium partners to provide their contributions and the peer review.

D8.1 Standardization Plan will be updated regularly within the duration of the project.

1.3 Standardization in a nutshell

In ISO/IEC Guide 2:2004¹, 1.1 standardization is defined as an activity of establishing, with regard to actual or potential problems, provisions for common and repeated use, aimed at the achievement of the optimum degree of order in a given context. Important benefits of standardization are improvement of the suitability of products, processes and services for their intended purposes, prevention of barriers to trade and facilitation of technological cooperation. Standardization supports the social and economic development by ensuring safety, quality and competitiveness of products, services and processes on various levels (e.g. performance, composition, interoperability, applicability and many more). This in turn supports economic activity of businesses of all sizes and allows them access markets all over the world.

Standardization is governed by the principles of consensus, openness, inclusiveness transparency, national commitment and coherence as outlined in the Agreement on Technical Barriers to Trade of the World Trade Organisation (WTO TBT Agreement) and in Regulation (EU) No

¹ ISO/IEC Guide 2:2004, Standardization and related activities — General vocabulary, is adopted in Europe as European Standard EN 45020:2006.

1025/2012 of the European Parliament and of the Council of 25 October 2012 on European standardisation.

The output of standardization are standards. According to ISO/IEC Guide 2:2004, 3.1 a standard is a document, established by consensus and approved by a recognized body, that provides, for common and repeated use, rules, guidelines or characteristics for activities or their results, aimed at the achievement of the optimum degree of order in a given context. Standards are voluntary in their application and should be based on the consolidated results of science, technology and experience, and aimed at the promotion of optimum community benefits. Standards are initiated and drafted by stakeholders such as industry, incl. SMEs, public authorities, research organisations, societal and environmental stakeholders, consumer organisations, trade unions and conformity assessment bodies.

There are numerous organizations developing standards, ranging from companies, consortia and industry in the private sector, to national, regional and international organizations. The latter three constitute the bulk of the international standardization system, required by the WTO TBT Agreement to follow its principles and requirements for standards development. There are also NGOs with specific socio-economic or environmental goals that develop and publish standards.

National Standardization Bodies (NSB) are standardization organizations located in each country. They bridge the local communities with groups of relevant stakeholders outside of their country and represent the pillars of the European and International standardization. Being member of European Standardization Organisations NSBs are obliged to implement European Standards as national standards and withdraw any conflicting national standards.

The European standardization activities are conducted within the European Committee for Standardisation (CEN), the European Committee for Electrotechnical Standardisation (CENELEC), and the European Telecommunications Standards Institute (ETSI).

CEN brings together the national standardization bodies of 34 European countries and provides a platform for standardization in various areas, including products, materials, services, and processes. CENELEC ensures standardisation in the electro-technical engineering field, and ETSI produces standards for information and communications technology.

The network of European standardization includes more than 200.000 experts from different countries and from the different stakeholders, i.e. business, industry and commerce, service providers, consumers, environmental and societal organisations, public authorities and regulators, as well as other public and private institutions. The European Standardization Organisations aim to support needs of the market and of different stakeholders, promoting the European Standardization System and leading the implementation of best practice in standardization around the world. They collaborate with key stakeholders' organisations at national, European and international level, support international Standardization and cooperate closely with international Standardization Organisation such as ISO and IEC. Participation in European

Standardization follows the national delegation principle, i.e. national members (NSB, NC) host national committees populated with national stakeholders and these national committees contribute to the elaboration of European Standards.

International standardization activities are conducted at three major international Standardization Organisation: International Organization for Standardization (ISO), International Electrotechnical Commission (IEC) and International Telecommunication Union (ITU).

ISO is an independent international organization that includes 165 national standards bodies as its members. International standards, produced by ISO, cover a wide variety of areas and represent consensus of experts from many countries. All CEN members are also members of ISO, with the Vienna Agreement ensuring transparency and exchange of information between them.

Members of IEC are 89 National Committees, represented by delegates from industry, research and government bodies of each country. IEC produces standards covering all aspects of production and use of electrical and electronic devices and systems. All CENELEC members are also members of IEC, their relationship being regulated by the Frankfurt Agreement.

ITU is an inter-governmental organization belonging to the United Nations and develops technical standards that facilitate the use of public telecommunication services and systems for communications in the area of ICT. Its membership comprises nearly 200 countries and almost 800 private-sector entities and academic institutions.

Participation in International Standardization of ISO and IEC follows the national delegation principle, i.e. national members (NSB, NC) host national committees populated with national stakeholders and these national committees contribute to the elaboration of International Standards.

A vast array of normative documents is classed under the generic label of "private standards". Generally, a normative document developed and published by an organization outside of the recognized standards development organizations at national, regional or international level is considered to be a private standard. There is not only a vast range of private standards (and growing in number), there are also significant differences between the bodies and organizations that develop these standards related to such aspects as governance, development approach, stakeholder engagement, transparency, and consensus. Some of these Private Standards Development Organisations liaise with recognized standards development organizations such as IEEE and ENISA liaising with ISO/IEC JTC 1/SC 27, Information security, cybersecurity and privacy protection or OASIS liaising with ISO/IEC JTC 1/SC 37/WG 2, Biometric technical interfaces.

1.4 Methodology

1.4.1 Overview of the standardization landscape

The content for the overview of the standardization landscape is based on a combination of resources, derived from standards databases of the European Committee for Standardization (CEN), European Committee for Electrotechnical Standardization (CENELEC), International Electrotechnical Commission (IEC), The International Organization for Standardization (ISO), European Telecommunications Standards Institute (ETSI), IEEE (Institute of Electrical and Electronics Engineers) and NIST (National Institute of Standards and Technology), as well as contributions from the consortium partners (mainly covering non-formal standards). The final standardization landscape covers thus European and international Standardization communities.

Initial literature review on the topic of cybersecurity in transport sector was conducted by Austrian Standards International. The broad areas of focus were first identified (cybersecurity, public transport, privacy, data management, cyber threats, infrastructure and equipment), followed by further classification according to the scope of the relevant standardization committees (e.g. personal identification devices, road equipment, applications for railway systems).

The database search was performed using the following keywords:

- Cybersecurity (incl. risk analysis methods and security assurance),
- cyberthreat,
- privacy,
- data protection,
- data management,
- smart city,
- public transport,
- intelligent transport,
- transport system.

In addition, the relevant technical committees of the European and International SBs were screened to identify relevant standards that could potentially be missed by the key words.

1.4.2 Analysis of standardization gaps and needs

A survey performed in English has been developed at ASI in order to collect missing standardisation elements and identify as many gaps as possible with the help of the project consortium. Since the nature of those missing elements can vary, they can be detected by experts from different areas.

The survey aimed to:

1. Identify the standards, regulations and frameworks used by the respondents
2. Reveal the areas that are lacking adequate standardisation from the point of view of the respondents
3. Identify any information (gaps) that the mentioned documents miss from the point of view of the respondents

4. Understand the shortcomings of the existing standards, as well as inadequacies of the existing training curricula

The survey is intended to provide qualitative information on standardisation gaps and mostly contains open-ended and multiple choice-questions. To cover all necessary legal aspects, the survey was complemented by an informed consent section, which was part of the survey and was presented to the respondent before the start. No personal information (i.e. name, e-mail address or phone number) was gathered, the respondents were only asked to name the organization they work in.

ASI distributed the survey among the CitySCAPE consortium members, who forwarded the link to their external partners to collect the largest possible spectrum of information.

The survey has been published online on 02.12.2020; the link to the survey was distributed on the same day. The deadline was set 10.01.2021, but the survey remains open to collect any possible inputs that could be provided later.

2 STANDARDIZATION LANDSCAPE

In addition to the survey among CitySCAPE partners, further standardization deliverables have been identified from ENISA reports² by ASI based on desk top research

In total, 534 relevant standardization deliverables have been identified so far, comprised of 520 formal and 14 non-formal standards.

After the initial survey, a second iteration among CitySCAPE partners was performed in February 2022. In this stage further standardization deliverables were identified, leading to an increase to 547 standardization deliverables (530 formal and 17 non-formal standards).

2.1 Formal standards

In Table 1 the identified formal standardization bodies with the number of relevant formal standards are listed.

Standardization body	Number of standards
CEN Workshop CIRRU	1
CEN/CENELEC JTC 13, Cybersecurity and Data Protection	4
CEN/TC 224, Personal identification and related personal devices with secure element, systems, operations and privacy in a multi-sectorial environment	8
CEN/TC 226, Road equipment	2
CEN/TC 278, Intelligent transport system	27
CLC/TC 9X Electrical and electronic applications for railways	3
ETSI TC ITS Intelligent Transport Systems	324
IEC TC 65, Industrial-process measurement, control and automation	10
IEC TC 79 - Alarm and electronic security systems	3
IEC TC 9 - Electrical equipment and systems for railways	11

² Such as the Compendium of Risk Management Frameworks with Potential Interoperability, January 13, 2022, <https://www.enisa.europa.eu/publications/compendium-of-risk-management-frameworks>, and Railway Cybersecurity, Security measures in the Railway Transport Sector, November 2020, <https://www.enisa.europa.eu/publications/railway-cybersecurity>

Standardization body	Number of standards
IEEE	9
ISO TC 241, Road traffic safety management systems	2
ISO/IEC JTC 1, Information Technology	1
ISO/IEC JTC 1/SC 17, Cards and security devices for personal identification	8
ISO/IEC JTC 1/SC 27, Information security, cybersecurity and privacy protection	26
ISO/IEC JTC 1/SC 37 Biometrics	1
ISO/IEC JTC 1/SC 38 Cloud computing and distributed platforms	1
ISO/IEC JTC 1/SC 41, Internet of things and digital twin	3
ISO/TC 204, Intelligent Transport Systems	68
ISO/TC 22 Road vehicles	1
ISO/TC 22/SC 32, Electrical and electronic components and general system aspects	2
ISO/TC 268, Sustainable cities and communities	3
ISO/TC 268/SC 1, Smart community infrastructures	9
ISO/TMBG Technical Management Board - groups	1
NIST	2

Table 1: Standardization bodies and number of formal standards

The formal standards are summarized in [ANNEX 2](#).

2.2 Non-formal standards

We have identified 17 non-formal standards, developed by CIS, Center for Internet Security, the UK Department for Transport, ENISA, MANDIANT, MobilityData, North American Bikeshare Systems Association (NABSA), OASIS Cyber Threat Intelligence (CTI), The Alliance for Parking Data Standards (APDS) and The MITRE Corporation. Furthermore, considering mobility services applications it seems suitable to mention also Syslog RFC 3164 for communication among devices (i.e., smartphones) and checking vulnerabilities and threats on each of them.

The formal standards are summarized in [ANNEX 3](#).

3 STANDARDIZATION GAPS AND NEEDS

3.1 Survey results

15 participants (consortium members as well as one representative of external stakeholders) have provided their responses. All of them contained answers to all questions, no partly filled surveys have been recorded.

Question 2: In your opinion, is identification of cybersecurity threats in the transport ecosystem addressed comprehensively? If not: Please indicate what improvements you suggest.

15 informative answers were provided to this question. Only three respondents (20%) agreed that identification of cybersecurity threats is comprehensively addressed, whereas 12 respondents (80%) identified a number of areas where improvements are needed and issues to be tackled:

1. Privacy-related threats
2. Specific treatment for cybersecurity threats
3. Mobile device threats detection and response, security awareness training and threat intelligence
4. New cybersecurity issues related to new technologies (e.g. electronic ticketing, mobile services)
5. Collaboration among all the involved stakeholders to improve information and knowledge sharing
6. Lack of specific security standards for transport ecosystem to support the management of specific threats
7. Lack of awareness of the technologies and security measures to be adopted to mitigate the risk associated with cyber threats
8. Lack of transparency between stakeholders
9. Strong conservatism of transport ecosystem

Question 3: What are the major shortcomings of the architecture of existing city transport ecosystem?

10 informative answers were provided to this question. The following shortcomings were identified:

1. Several actors are involved (customers, industry) with no specific requirements
2. No specific processes are set up to address cybersecurity; audit is only done when issues are raising
3. Lack of consideration of the 'security by design' paradigm
4. Lack of integration, stratifications of different technology "eras"
5. Security is neither included in the initial specification nor in the acceptance tests
6. Inadequate communication among moving transport and central systems
7. Minor emphasis on the collaboration and communication with all the involved actors.
8. Limited adoption of new interoperability approaches and protocols
9. Inadequate integration of Legacy System and Open Data
10. Lack of an appropriate data management system (no widely adopted language to model the system of systems)

11. Superficial evaluation that leads to underestimation of certain threats and improper security measures
12. Lack of proper planning and organization of the security measures that lose their effectiveness over time
13. No real consideration of cyber risk
14. Lack of a holistic view due to the presence of several independent monitoring systems

Question 4: What are your main concerns regarding data handling within the transport ecosystem?

12 informative answers were provided to this question. The following concerns were identified:

1. Leakage of data to third parties
2. Susceptibility of data to attacks, corruption and misuse
3. Inadequate protection of data transmission and storage of data on servers
4. Inadequate coverage of user data privacy and security in all processes.
5. Inadequate communication, including mobile communication and provision of traffic information to customers
6. Inadequate adoption of and compliance of data processing with GDPR and ethics
7. Lack of a common terminology
8. Difficulties working with open data to generate applications that use it, and increase its value

Question 5: Are the training needs for cyber security experts in the transport sector appropriately covered by the existing training curricula?

11 informative answers were provided to this question. Only one respondent found the coverage of the training needs adequate, whereas 10 respondents identified the following deficiencies:

1. Lack of a tailored training for security and privacy of transport sector stakeholders
2. Lack of focus on cybersecurity in public transport in expert curricula
3. Inadequate addressing of new incoming cyber threats and of a new cyber/physical dimension in expert curricula
4. The transport-related topics are not currently very relevant, but they will become so in the nearest future

Question 6: Please provide examples of existing training curricula

10 informative answers were provided to this question. Among them, one respondent stated that there is no specific training curriculum. The provided examples include:

1. National Initiative for Cybersecurity Careers and Studies (US based)
2. <https://www.k-asap.com/en/>
3. <https://www.proofpoint.com/us/wombat-security-is-now-proofpoint>
4. <https://www.knowbe4.com/>
5. UNI-EN related certification training curricula and specific training on specific product used

6. IOT cybersecurity courses
7. Specific university courses in the field of cyber security, both degree and masters' courses.
8. ENISA best cyber security practices publications

Question 7: Are you using cybersecurity standards in your work efforts? If yes: Which of the following areas do these standards cover (System Architecture, System Requirements, Interoperability, Data Handling, Training, other)?

Five respondents (33,3%) did not use cybersecurity standards, whereas 10 respondents (66,7%) used standards covering the following proposed areas:

1. Software development
2. Data Handling
3. System Architecture
4. Interoperability
5. System Requirements

In addition, the option "other" included the areas covered by the Mitre Att&ck Framework, as well as the areas of infrastructure security, policies for personnel and users, cyber security mechanisms.

Question 8: Please name the standards you use the most

9 informative answers were provided to this question. The standards used the most include:

1. HyperText Markup Language (IETF, ISO, W3C) or HTTP
2. ECMAScript (ECMA, ISO)
3. JavaScript Object Notation
4. Structured Query Language (ANSI, ISO)
5. SSL
6. SIRI
7. Mitre Att&ck
8. NIST best practise
9. CEN Transmodel
10. NeTEx group of standards:
 - a. CEN/TS 16614-1:2014 Public transport - Network and Timetable Exchange (NeTEx) - Part 1: Public transport network topology exchange format
 - b. CEN/TS 16614-2:2014 Public transport - Network and Timetable Exchange (NeTEx) - Part 2: Public transport scheduled timetables exchange format
 - c. CEN/TS 16614-3:2016 Public transport - Network and Timetable Exchange (NeTEx) - Part 3: Public transport fares exchange format
11. ETSI TR 102 893 Intelligent Transport Systems (ITS); Security; Threat, Vulnerability and Risk Analysis (TVRA)
12. ISO/IEC 27001:2013 – Information technology – Security techniques – Information security management systems – Requirements
13. ISO 31000:2018 Risk Management — Guidelines
14. ISO 31010:2019 Risk management — Risk assessment techniques
15. ISO 27032:2012 Information technology — Security techniques — Guidelines for cybersecurity

Question 9: Do you see any gaps in the current cybersecurity standards in the city transport ecosystem? If yes: Which of the following areas do these standards cover (System Architecture, System Requirements, Interoperability, Data Handling, Training, other)?

Five respondents (33,3%) have not found any gaps in the cybersecurity standards, whereas 10 respondents (66,7%) identified standardization gaps in all provided areas. Such areas as Data Handling, System Architecture and Interoperability were mentioned several times.

In addition, one respondent suggested that the findings from the Cybersecurity Standard Gap Analysis [1] are valid also in the city transport ecosystem. These findings will be explored further in the Section 3.2 Standardization focus points for the CitySCAPE consortium. **Error! Reference source not found. Error! Reference source not found.**

Question 10: Could you name the most urgent standardization gaps?

8 informative answers were provided to this question. The most urgent standardization gaps were identified as follows:

1. The link between data (e.g. handling, integrity) and functional safety
2. Lack of common language in cyber risk management processes
3. Lack of integration between Business-Critical processes and cyber security processes
4. Passenger data processing and handling
5. Real time operational bus data
6. System architecture definition and interoperability specification
7. Lack of widely adopted language and methodology to model the whole transport infrastructure
8. No official standard on cybersecurity risk linked to multi-modal transport

Question 11: What are your greatest concerns regarding the existing cybersecurity standards? (f.e. which standard to use, usability, coherence between different standards, too generic, complexity of standards, lack of an appropriate standard, other)

13 informative answers were provided to this question. The greatest concerns regarding the existing cybersecurity standards included:

1. Complexity of cybersecurity in public transport system
2. Lack of appropriate standards in certain areas
3. Lack of best practices in available standards to make them implementable in a production environment
4. Too many standards and lack of a consensus on which standard to use
5. Lack of awareness about standards in the PT domain
6. Lack of coherence between different standards
7. Need of a single standard that horizontally refers to already existing standards that cover different domains on different levels
8. Absence of an appropriate standard linked to the multi-modal transport network and the risks that this will generate (e.g. the risk of updates (OTA), the dialogue between vehicles (V to V) and between vehicle and road infrastructure (V to I)

9. Certain standards are too generic

Question 12: Are your city multimodal systems compliant with transport European data exchange standards (Transmodel, SIRI, NeTEx)?

Three respondents (20%) stated that their city multimodal systems are not compliant with transport European data exchange standards, four respondents (26,7%) confirmed such compliance. Eight respondents indicated that the question was not applicable to their situation.

All responses are presented in [ANNEX 1](#).

3.2 Standardization focus points for the CitySCAPE consortium

Based on the information derived from the Standardization Gaps and Needs Survey, the most important focus points for future standardization activities can be identified as follows:

1. Data management
 - a. Handling of all passengers-related data
 - b. Management of real-time operational data between vehicles and between vehicles and infrastructure
2. Common language for cyber risk modelling and management
3. Integration of cybersecurity processes into system architecture to ensure its alignment with business-critical processes
4. Development of a specific overarching cybersecurity standard for multi-modal transport that integrates/refers to already existing standards

4 STANDARDIZATION PLAN

4.1 General

Based on the survey on standardisation (in Section 3), the standardisation plan devised in the project is based on the PDCA (Plan – Do – Check – Act) methodology. This involves pursuing the following activities:

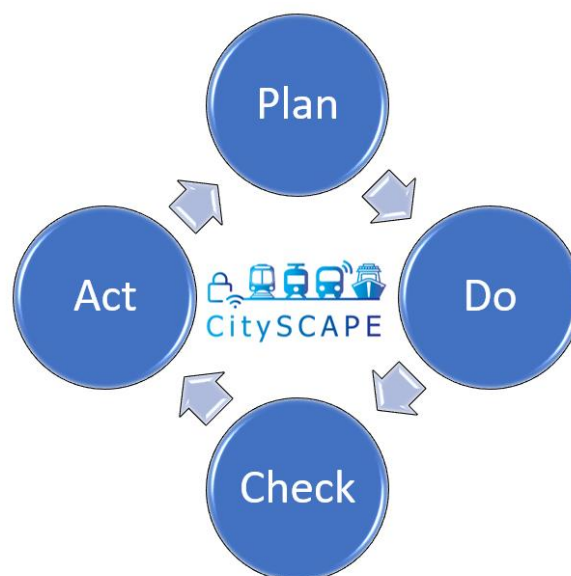


Figure 1: PDCA methodology for the CitySCAPE standardization plan

- **Phase Plan:**
Based on the surveys in Section 3, a decision on standards relevant for the project is carried out.
- **Phase Do:**
The project partners ensure the compatibility and interoperability of their services and technical solutions with the relevant standards. Partners contribute towards the compliance, application, and development of standards in the areas of relevance to CitySCAPE as follows (see Section 3.2):
 - Data management;
 - Handling of all passengers-related data;
 - Management of real-time operational data between vehicles and between vehicles and infrastructure;
 - Common language for cyber risk modelling and management;
 - Integration of cybersecurity processes into system architecture to ensure its alignment with business-critical processes;
 - Development of a specific overarching cybersecurity standard for multi-modal transport that integrates/refers to already existing standards.

Project partners contribute to activities in Standards Development Organisations (SDOs) working on cybersecurity standards for multi-modal transport ecosystems (see Section 4.3).

- **Phase Check:**
Partners, especially those involved in WP5, WP6 and WP7, shall periodically review and align their standardisation activities and provide a report for internal and external awareness. The findings will be used to update D8.1 regularly within the duration of the project.
- **Phase Act:**
If the new subject areas relevant to the project are planned or identified by SDOs (e.g. CEN, CENELEC, ETSI, IEC, ISO, IEEE) the partners have to create a corresponding analysis of the target status and compare it with the current status. Furthermore, the questions of what can be optimized and where lay a further potential of standardization activities (see Section 4.3) must be clarified. If it is determined that the goal has not been reached, the cycle is run through again.

4.2 Strategic Areas of Participation

The analysis of the ongoing standardisation activities in the project and partners interests reveals the following key areas that require an active participation from a project's strategic point of view.

Those partners participating in the following standardisation areas are committed to report latest and important developments to the project and feed findings from the project back to standardisation. Such two-way interaction between CitySCAPE and standardization communities contributes to an optimal alignment of the project activities and outcomes with standards (published and under development).

Special attention needs to be given to those standardisation projects, which support regulations. Especially New Legal Framework (NLF) directives/regulations of the European Union foresee a strong link with standards. These standards are elaborated based on a standardisation request from the European Commission and gain the status of harmonized European Standards (hEN). Such NLF regulation is, for instance Directive 2010/40/EU of the European Parliament and of the Council on the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other modes of transport.

In case, no other partner participates in a standardization body listed below, ASI as member of CEN, ISO, ETSI and having contacts with CENELEC and IEC will be used as communication channel.

4.2.1 CEN/TC 278, Intelligent transport system

The scope of CEN/TC 278 is the standardization in the field of intelligent transport systems, encompassing services and techniques to achieve road safety, environmental sustainability and traffic efficiency, and to improve the

travel experience; applying information and communication technologies between vehicles/infrastructure/other road users.

The following are included in the scope of CEN/TC 278:

- aspects of cooperation (C-ITS);
- intermodality and multimodality;
- traffic management;
- mobility information;
- mobility integration;
- mobility as a service;
- systems and services for vulnerable road users;
- ITS services for automated vehicles;
- parking management;
- user fee collection;
- public transport management;
- eCall;
- after-theft vehicle recovery systems;
- kerbside and pavement management.

Mobility accessibility for all users is an important aspect of ITS standardization.

CEN/TC 278 cooperates with the international standardization committee ISO/TC 204, Intelligent transport systems, in the framework of the Vienna Agreement to transport relevant international standards as European Standards (ENs).

CEN/TC 278 is the responsible standardization committee for the multi-part European Standard **EN 12896**, *Public transport - Reference data model*. This standard is not directly used in CitySCAPE labelling work, i.e. **Task 8.2** Standardization Activities in support of a security labelling for transport (**CSG**), because it defines a conceptual model. On the other hand, systems implementing SIRI & NeTEx standards should comply with them as they use the same concepts. Transmodel contributes to the design of scalable and interoperable transport systems refer to the different parts of the standard, i.e.

- Part 2: Public transport network
- Part 3: Timing information and vehicle scheduling
- Part 4: Operations monitoring and control
- Part 5: Fare management
- Part 6: Passenger information
- Part 7: Driver management
- Part 8: Management information & statistics

Another European Standardization deliverable in the scope of CEN/TC 278 is multi-part **CEN/TS 16614**, *Public transport - Network and Timetable Exchange (NeTEx)*. NeTEx is included in the study carried out as part of **Task 8.2** Standardization Activities in support of a security labelling for transport (**CSG**). Its evaluation with regard to cybersecurity threats and in the implementation of a labelling process are integrated into the study. NeTEx is unavoidable (mandatory) within the framework of the EU-Directive 2010/40 on the framework for the deployment of Intelligent Transport

Systems in the field of road transport and for interfaces with other modes of transport, Action A. Nevertheless, within the framework of CitySCAPE, particular attention is paid to Part 1, *Public transport network topology exchange format*, which defines the common mechanisms for the exchange of information (identification of subscriptions, requests, etc.)

The multi-part European Standard **EN 16157**, *Intelligent transport systems - DATEX II data exchange specifications for traffic management and information*, is a standard centred on road traffic which does not fall directly within the scope of **Task 8.2**, Standardization Activities in support of a security labelling for transport (**CSG**). However, the information it conveys may relate to transport systems (route search). The services provided by this standard will be considered in **Task 8.2**.

The multi-part European Standard EN 15531, *Public transport - Service interface for real-time information (SIRI) relating to public transport operations*, is integrated into the study carried out as part of **Task 8.2** Standardization Activities in support of a security labelling for transport (**CSG**). Generic mechanisms will be integrated into this analysis.

CSG participates in CEN/TC 278.

4.2.2 ISO/IEC JTC 1/SC 27, Information security, cybersecurity and privacy protection

ISO/IEC JTC 1/SC 27 is the responsible standardization committee for **ISO/IEC 27001**, Information technology — Security techniques — Information security management systems — Requirements. This International Standard has been adopted as European Standard (EN ISO/IEC 27001). On European level [CEN-CLC/JTC 13](#) 'Cybersecurity and data protection' has the primary objective to transport relevant international standards (especially from ISO/IEC JTC 1/SC 27) as European Standards (ENs) in the Information Technology (IT) domain. It also develops 'homegrown' ENs, where gaps exist, in support to EU regulations (RED, eIDAS, GDPR, NIS, etc.). These two streams of activities aim at creating a strategic portfolio of standards in Europe, which fits the European needs. CEN-CLC/JTC 13 works closely with ENISA (The European Union Agency for Cybersecurity) in the context of the European certification schemes, and with the European Commission, in the frame of the cybersecurity-related standardization request under the Radio Equipment Directive (RED).

The *MobSec* mobile App defined in **Task 3.3 (ED)**, Secure multi-modal transport architectures, and implemented by SIGLA to build a 'secure by design' mobile app for passengers of multimodal local transport is integrated with Kaspersky Mobile Security SDK (KMS-SDK) (**KSP**). The Collaborative Threat Intelligence Platform (CTIP) defined in Task 3.3 and implemented by AIRBUS is fed by the Kaspersky Threat Data Feeds. KMS-SDK and Kaspersky Threat Data Feeds are based on services provided by the Kaspersky Security Network (KSN). KSN is ISO/IEC 27001 certified in the delivery of malicious and suspicious files.

ENG follows ISO/IEC 27001 through the adoption of the best practices on information security and in particular on information security management systems, from the definition of requirements to the development of all solutions.

Application of ISO/IEC 27001 to multimodal CPaaS transport system is taken into account as part of **Task 8.2**, Standardization Activities in support of a security labelling for transport (**CSG**).

ED uses ISO/IEC 27001 as a guide for the specification of the Design and Implementation of RITA, which is considered a well-documented Information Security Management System (ISMS). Although RITA follows an asset-based risk assessment the tool follows a process-based approach, in line with the model proposed by ISO/IEC 27001.

Regarding **ISO/IEC 27002**, *Information technology — Security techniques — Code of practice for information security controls*, which is also adopted as European Standard, **ACS** leverages this code of practice in the design of all its solution to ensure a high level of security is attained. Application of ISO/IEC 27002 to multimodal CPaaS transport system is taken into account as part of **Task 8.2**, Standardization Activities in support of a security labelling for transport (**CSG**).

Additionally to CIS Controls **ED** leverages the basic concepts introduced by ISO/IEC 27002, i.e. policy, safeguard or control or countermeasure, risk and information security incident, and through RITA assists organizations to build appropriate countermeasures that when applied help protect their information systems. These controls follow the categorization established in ISO/IEC 27002.

ACS leverages **ISO/IEC 27003**, *Information technology — Security techniques — Information security management systems — Guidance*, in the design of all its solution to ensure a high level of security is attained. **ED** uses ISO/IEC 27003 towards the implementation of RITA, which can be used by organisations towards establishing, implementing, monitoring, reviewing, maintaining, and improving their information security in order to achieve their business objectives. RITA is based on a risk assessment and is designed to effectively identify, treat, and manage risks. RITA supports the implementation and operation of security measures, appropriate to deal with risks that fall within the specific organizational framework. RITA supports different roles and supports both the information security risk assessment and information security risk treatment by identifying and implementing controls.

ED uses the methodology provided in **ISO/IEC 27005**, *Information technology — Security techniques — Information security risk management*, to help organisations manage their risk. It uses the established definition of risk, i.e. function of probability and impact as well as the related concepts including assets, threats and vulnerabilities. RITA as a risk management tool supports both risk assessment (risk identification,

analysis and evaluation) and risk treatment phases of risk management. To support with the preparation of a security plan, RITA allows the definition and selection of countermeasures, controls, safeguards.

ED uses **ISO/IEC TS 27008**, *Information technology — Security techniques — Guidelines for the assessment of information security controls*, as a complementary text to the information security risk management process described in **ISO/IEC 27005** in the design of RITA, in order to enable organisations using RITA to select countermeasures that are fit for purpose, effective and efficient. Essentially, the process of evaluating technical countermeasures according to ISO/IEC TS 27008 is part of ISO/IEC 27002, discussed above.

Application of **ISO/IEC 27009**, *Information security, cybersecurity and privacy protection — Sector-specific application of ISO/IEC 27001 — Requirements*, to multimodal CPaaS transport system is taken into account as part of **Task 8.2**, Standardization Activities in support of a security labelling for transport (**CSG**), to create an ISO/IEC 27001 extension dedicated to urban transport systems

ENG will apply **ISO/IEC 27039**, *Information technology — Security techniques — Selection, deployment and operations of intrusion detection and prevention systems (IDPS)*, in **Task 5.4**, IDS/IPS engines (**ENG**), for the development of CITYSCAPE IDS/IPS.

In **Task 8.2**, Standardization Activities in support of a security labelling for transport (**CSG**), multi-part standard **ISO/IEC 15408**, *Information technology — Security techniques — Evaluation criteria for IT security*, which is also adopted as European Standard, is taken into account as part of the labelling process to be defined. The same applies for **ISO/IEC 18045**, *Information technology — Security techniques — Methodology for IT security evaluation*.

OPP is an ISO/IEC 17025, *General requirements for the competence of testing and calibration laboratories*, accredited Information Technology Security Evaluation Facility (ITSEF) for **ISO/IEC 15408-1:2009**, *Information technology — Security techniques — Evaluation criteria for IT security*. To perform these evaluations, **OPP** uses the associated evaluation guidelines defined in ISO/IEC 18045, *Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Methodology for IT security evaluation*.

CC is a well-known and established approach to evaluate a specific product in a specific version. **OPP** performs several CC evaluations every year that last month's up to years for the most complex products. In the context of CitySCAPE, since multimodal systems are composed of hundreds see thousands of different products, **OPP** has developed a new assurance methodology based on CC but is more adapted and thus efficient to the multimodal systems ecosystems. So, **OPP** has used both CC during the project and outside the project for its regular services.

Also, **OPP** provides many audit services for a large variety of costumers. To provide more harmonized and recognized audit results, several regulatory contexts impose to use **ISO/IEC 27001**, **ISO/IEC 27002** or **ISO/IEC 27005** references. For instance, **OPP** has audited European ITS KPI services using **ISO/IEC 27001** as a basis as well as many French Critical Infrastructure and services.

ENG participates in ISO/IEC JTC 1/SC 27 and CEN-CLC/JTC 13.

4.2.3 NIST

The *MobSec* mobile App defined in **Task 3.3 (ED)**, Secure multi-modal transport architectures, and implemented by SIGLA to build a 'secure by design' mobile app for passengers of multimodal local transport is integrated with Kaspersky Mobile Security SDK (KMS-SDK) (**KSP**). KMS-SDK encrypts internal product data files and security requests to KSN following Advanced Encryption Standard AES 256.

OPP regularly evaluates products including well known cryptographic functions, **FIPS 140-2** has been used by us as one state of the art reference for crypto modules functional testing. This standard provides an important conformity data base that can be useful in some context where conformity of specific implementation must be tested. This standard as also been used as an input for operational assurance approaches to develop conformity tests tools to be used in real operational environments.

4.2.4 MobilityData

Since organizations that work with highly detailed data internally using standards like NeTEx find *The General Transit Feed Specification (GTFS)* useful as a way to publish data for wider consumption in consumer applications, **GTFS** and **GTFS RealTime** are fully integrated to **Task 8.2**, Standardization Activities in support of a security labelling for transport (**CSG**), as it is widely implemented as part of transport system interfaces.

The application **SIGLA** Moving is modular and natively very flexible letting to adapt the services that can be delivered case to case (i.e., PTO to PTO, City to City) making possible to tailor the services provided in parallel to the actual possibilities and IT infrastructure of each PTO. It focuses on interoperability and integrability by default, making possible to use the same app for multiple PTO and mobility services at the same time. In practice, the app can be adopted by many cities at the same time, enabling a user to travel on multiple cities (through different PTOs) without changing application or installing many on their phone. The app is natively multi-lingual and can be adopted independently to travel on different countries' PTOs' services. The solution provides the possibility of accessing info-mobility services (e.g., checking tickets validity, creating tickets, custom alerting/notifications, etc.) also for PTOs' staff dedicated to deliver those services. Hereafter the Non-Formal standards used for each considered PTO and for which interoperability has been tested:

- AMT (Genova, Italy): proprietary format returned by their API
- TLT (Tallin, Estonia): proprietary format returned by their API
- FOLI (Finland): standard GFTS
- HSL (Finland): standard GFTS
- LSL (Finland), standard GTFS
- Nysse (Finland), standard GTFS
- ATAC (Rome - Italy), standard GTFS
- TTE (Trento - Italy), standard GTFS

Gruppo SIGLA doesn't participate in the work of this standardization activities.

Regarding General Bikeshare Feed Specification (**GBFS**), this is integrated as part of Transport standards to be studied as part of **Task 8.2**, Standardization Activities in support of a security labelling for transport (**CSG**).

4.2.5 OASIS

ACS leverage *Structured Threat Information eXpression (STIX 1.4 and 2.0)*, developed in OASIS Technical Committee on Cyber Threat Intelligence (CTI), inside the CTIP component to store IOCs and their contextualization data into a MISP instance. Some limitations of the model have been bypassed by upgrading the model specifically.

The Collaborative Threat Intelligence Platform (CTIP) defined in **Task 3.3**, Secure multi-modal transport architectures (**ED**), and implemented by AIRBUS is fed by the Kaspersky Threat Data Feeds (**KSP**). The Kaspersky Threat Data Feeds list of Indicators of Compromise (IOCs) is available in standard formats like STIX.

4.2.6 The MITRE Corporation

The **MITRE ATT&CK framework** is not used by default inside the CTIP component, but **ACS** has designed a solution that is compatible with it through the integration of commonly available plugins.

When **OPP** providing cyber-security services, the problem of using commonly accepted taxonomies to normalized services results is important. Among many other needs, **OPP** customers often require classifying identified system or product weaknesses. Very few such taxonomies have wide recognition. One of them worth to be mentioned and regularly used by **OPP** is the Common Weaknesses Enumeration database defined by the **MITRE**. This data base presents and defines one of the most precise and exhaustive cyber-security weaknesses taxonomy, even if several criticisms can be made about its content (inconsistency of weakness description precisions or examples provided, redundancy, etc.).

4.2.7 MANDIANT

The *Open Indicators of Compromise (OpenIOC) Framework* is not used by default inside the CTIP component, but **ACS** has designed a solution that is compatible with it through the integration of commonly available plugins.

The Collaborative Threat Intelligence Platform (CTIP) defined in **Task 3.3**, Secure multi-modal transport architectures (**ED**), and implemented by AIRBUS, is fed by the Kaspersky Threat Data Feeds (**KSP**). The Kaspersky Threat Data Feeds list of Indicators of Compromise (IOCs) is available in standard formats like OpenIOC.

4.2.8 ENISA

ENISA's **Cybersecurity Certification: EUCC Candidate Scheme** is part of **Task 8.2**, Standardization Activities in support of a security labelling for transport (**CSG**), i.e. the labelling process analysis and definition.

4.2.9 Syslog

Cyber-security is a must-have nowadays to protect the delivery and the access to all info-mobility services. Within CitySCAPE, **SIGLA** faces this issue enforcing cyber-security thanks to the integration of Kaspersky Mobile Security SDK providing “security by design” into the actual infrastructure of SIGLA Moving application. Furthermore, SIGLA used **RFC 3164** standard in communication with SIEM, relating to threats and vulnerabilities found on individual devices.

Gruppo **SIGLA** participates in the work of Syslog.

4.2.10 Center for Internet Security (CIS)

ED, **STAM** and **ENG** leverage **CIS Critical Security Controls** to build the set of countermeasures that the organization can apply to protect its information systems. CIS controls can be selected in FIMCA as possible security measures for the organization under analysis. Each CIS control has mitigation factors that counteract the threats it may face, and the cost associated with implementing them. These controls are also leveraged by **ED** and **UPRC** to assess the organization's residual risk in RITA and by FIMCA to assess financial impact.

The **CIS** benchmarks are regularly used by **OPP** has a reference set of requirements to be verified while performing technical security audits. CIS benchmarks proposes a wide and complete range of security configuration and recommendations for several technical platforms (windows, Linux, VMware, openstack, etc.).

4.3 Contribution to standardization

Project partners were asked to provide information about their participation in those standardization committees/organisations operating in domains being identified as strategic areas (in Section 4.2 this information is indicated as well):

- **CSG** participates in CEN/TC 278,
- **ENG** participates in ISO/IEC JTC 1/SC 27 and CEN-CLC/JTC 13, and
- Gruppo **SIGLA** participates in the work of Syslog.
- **ASI** as national standards body and member of CEN, ISO and ETSI is mirroring the activities of CEN/TC 278, Intelligent transport system, ISO/TC 204, Intelligent transport systems, CEN-CLC/JTC 13, Cybersecurity and data protection, and ISO/IEC JTC 1/SC 27, Information security, cybersecurity and privacy protection.

Project partners were also asked to provide information whether they have encountered any hurdles when implementing the standards mentioned in 4.2 in the project activities. The information received will be communicated to the appropriate standardization committee/organisation either by those who participate in them or by ASI. For this it is necessary to understand, that standards are subject to a systematic review process to ensure that they remain up-to-date and relevant. European and International standards (i.e. those from CEN, CENELEC, ISO and IEC) are reviewed at least every five years after publication by the users of the standard who have to provide the recommendation, either

- to confirm the standard (retention without technical change),
- to revise or amend the standard (retention with technical change), or
- to withdraw the standard because the standard does not reflect current practice or research, it is not suitable for new and existing applications (products, systems, or processes), or it is not compatible with current views and expectations regarding quality, safety, and the environment.

This systematic review process will be applied by CitySCAPE to provide the contribution for existing standards to the respective standardization committee including the information in the case when no obstacle was identified which can be seen as an indication to confirm the standard.

Only the following standards were identified with obstacles to implementation in the project activities:

- **CSG** reported, that for the implementation of EN 15531, *Public transport – Service interface for real-time information (SIRI)*, and CEN/TS 16614, *Public transport - Network and Timetable Exchange (NeTeX)* a good understanding of TRANSMODEL concepts is required and a TRANSMODEL training session is highly recommended before implementing these standards, which is already subject of the EU project DATA4PT³ (grant agreement No MOVE/B4/SUB/2019-

³ <https://data4pt-project.eu/>

104/CEF/PSA/SI2.821136). Since **CSG** participates in CEN/TC 278, where these standards have been elaborated and are maintained, **CSG** is committed to inform this CEN Technical Committee about this need.

- Gruppo **SIGLA** participating in the work of SYSLOG, re-empathized that for the exchange of data among CitySCAPE elements (from Mob-Sec to SIEM) adherence to standards is necessary.
- **ENG** reported, that CIS (Center for Internet Security) Critical Security Controls data was initially only available as Excel spreadsheet and therefore, the data feed could not be automated with new updates from CIS. It is recommended to have a look at the recent more machine-friendly version of the CIS Controls represented using the Open Security Controls Assessment Language (OSCAL) format. An introduction to this topic is available at <https://www.cisecurity.org/insights/blog/introducing-the-cis-controls-oscal-repository> and the actual OSCAL repository is available at https://github.com/CISecurity/CISControls_OSCAL.

Next to the contribution to existing standards another contribution to standardization are the standardization activities in support of a security labelling for transport. The recommendations elaborated in Task 8.2 (lead by **CSG**) and to be included in Deliverable D8.2, *Recommendations and options for a security labelling for transport*, will be provided as a candidate for a new work item proposal (NWIP) for elaborating a new standard either to CEN/TC 278, Intelligent transport systems, or CEN/CLC/JTC 13, Cybersecurity and Data Protection.

5 CONCLUSION

Based on a survey, gaps and needs as well as standards (published and under development) were identified for the project to facilitate market uptake of the developed solutions. This document outlines the standardization roadmap in the area of cybersecurity in transport system, the description of the actions for the focus areas of strategic participation in standardization and application of standards in the project as well as which partners participate in which standardization organisations, and which are the contributions to these standardization organisations.

As an added value, demonstrating which standards are applied in the project, respectively on which standards the solutions developed by CitySCAPE are based, enhances the market uptake of these solutions. This is because standards are recognized, trusted and used by the market and products or services complying with standards create customer gains and alleviate customer pains.

6 REFERENCES

- [1] Cybersecurity standard gap analysis. White Paper. Retrieved from https://cyberwatching.eu/sites/default/files/White-Paper-Cybersecurity-Standard-Gaps-Analysis_Cyberwatching.eu-October2018.pdf.
- [2] ENISA Compendium of Risk Management Frameworks with Potential Interoperability, January 13, 2022. Retrieved from <https://www.enisa.europa.eu/publications/compendium-of-risk-management-frameworks>.
- [3] ENSA, Railway Cybersecurity, Security measures in the Railway Transport Sector, November 2020. Retrieved from <https://www.enisa.europa.eu/publications/railway-cybersecurity>

ANNEX 1: GAP ANALYSIS SURVEY WITH RESPONSES

Title: CitySCAPE WP8: Standardization and Exploitation: Standardization Gaps And Needs

Introduction and foreword for the respondents

This survey is intended to reveal the needs of the CitySCAPE consortium partners with regard to standardization, as well as the gaps in the current standardization landscape that will be filled by the standardization activities within the project.

Informed consent

Your data will be protected and kept safe throughout this project and accessed and analysed by the researchers for the purpose of conducting this project. Data provided by participants will be stored for the duration of the project and kept 5 years after its final payment. The recipient of the personal data provided during this survey is Austrian Standards International, the National Standardization Body of Austria (<https://www.austrian-standards.at/home/>), which will process your data.

1. Please indicate your organization [open-ended]

- Institute of Communications and Computer Systems (ICCS)
- CS GROUP
- Kaspersky
- AMT Genova
- Aurige
- Engineering Ingegneria Informatica S.p.A.
- EURECAT
- Airbus CyberSecurity (ACS)
- CyberLens

2. In your opinion, is identification of cybersecurity threats in the transport ecosystem addressed comprehensively? [multiple choice and open-ended]

a. Yes

b. No: Please indicate what improvements you suggest

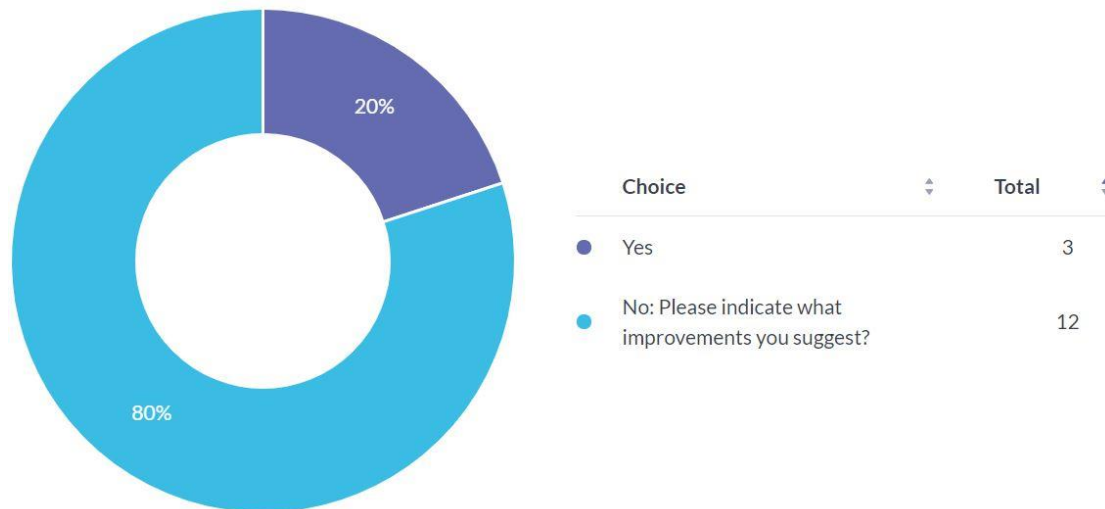


Figure 2: responses to question 2

Suggested improvements:

- a. Privacy threats seem to need further elaboration. The way threats are "shaped" as the automation level increases is also under-explored
- b. There is no specific treatment for Cybersecurity threats in transport ecosystem. This issue has never been analysed under this point of view
- c. Mobile device threats detection and response, security awareness training and threat intelligence can be improved
- d. Better understanding of the new cybersecurity issues related to new technologies such as electronic ticketing and mobile services
- e. PT is most often focused on Operation and Information... and often forget security as one of the requirements (at specification level)
- f. Cybersecurity threats need to be identified within a much more complex and variable landscape where everyday there are new vulnerabilities and new unknown threats to be taken into account. In that view, an improved collaboration among all the involved stakeholder allow information and knowledge sharing is strongly recommended
- g. In my opinion there is a lack of specific security standards for transport ecosystem to support the management of specific threats. Generic standards, such as the ISO27000 series, are not sufficiently useful for the complex reality of transport system and are poorly related to the security environment within transport organizations interact and operate today.
- h. The digitization of processes affects transport companies all over the world, but in reality not all companies are fully aware of the technologies and security measures to be adopted to mitigate the risk associated with cyber threats
- i. Transport ecosystem is too conservative, and it is difficult to reach some developments.

- j. More transparency and threat intelligence are needed between stakeholders.

3. What are the major shortcomings of the architecture of existing city transport ecosystem? [open-ended]

- a. Actual shortcomings are more and more covered by the new RFP, especially by identifying cybersecurity stakes and associated requirements. Actually: several actors are involved (Customer, industry) with no specific requirements; no specific processes are set up to address cybersecurity; audit are only done when issues are raising. Usually cybersecurity threat are addressed by the customer infrastructure.
- b. They usually involve legacy systems not having taken into consideration the 'security by design' paradigm. The cost of an attack is very low, if compared with the valuables that can be stolen by a criminal.
- c. Lack of integration, stratifications of different technology "eras"
- d. There are plenty, but just look at scalability and DDoS protection: most passenger information systems can easily be killed by a very simple DDoS (it can be a simple app making too many request... so you can imagine what hacker can do!). The major shortcomings is just that security is not in the initial specification nor in the acceptance tests
- e. communications among moving buses and central systems
- f. Minor emphasis on the collaboration and communication with all the involved actors.
- g. Limit in the adaption of new interoperability approaches and protocols
- h. Integration of Legacy System and Open Data
- i. Transport system is a complex ecosystem comprising hundreds of connected systems with a wide range of functions. Information exchange is the core of the transport ecosystem. Data is used for making traffic flow efficient, improving road safety, increasing revenue, and reducing ecological and environmental impact, among other uses. Data is also consumed by the users to improve their transit options and experiences. The main shortcoming is the lack of a management system. There is no a widely adopted language to model the system of systems.
- j. In some cases the transport companies consider some risks superficially based on what is the experience of the managers. This means that some threats are underestimated and that therefore some security measures are not properly applied, thus creating vulnerabilities that can be exploited to carry out the attack successfully. Furthermore, there is often a lack of proper planning and organization, which means that the security measures implemented lose their effectiveness over time.
- k. Currently, there is no real consideration of cyber risk

- l. There are several independent monitoring systems that make it difficult to have a holistic view.

4. What are your main concerns regarding data handling within the transport ecosystem? [open-ended]

- a. Leakage of data to third parties
- b. Data corruption, Malicious used, Access account blocked
- c. Data handling should take privacy into consideration not only in security plans but in all processes involving user data and in the staff trainings.
- d. Possible frauds or misuse of data
- e. 1/ keep the service running 2/ optimise and keep the cost as low as possible 3/ passenger information Security should be in 1/ but is often forgotten
- f. Mobile communications, traffic information to customers
- g. (1) Adoption and compliance with GDPR and ethics (2) Lack of a common terminology
- h. The data handling within the transport ecosystem are susceptible to attacks that can compromise roadway safety, especially when vehicles depend on transport system data for making critical driving decisions. Examples: The received/forwarded data may not be true; an attacker vehicle can generate false data. Vehicles can broadcast fake location data. This is a serious problem because safety-related applications/systems that rely on accurate vehicle location data will respond incorrectly. By simulating false driving conditions, attackers can deceive in-vehicle sensors, by braking repeatedly over a short distance, the attacker can simulate a traffic jam on the road, and the car can incorrectly broadcast a traffic jam message. Another issue is related to the operation of the transport system.
- i. The problems affecting the transport ecosystem are the same as those affecting any system that handles sensitive data. In some cases, the transmission of data is not adequately protected, thus jeopardizing the integrity and confidentiality of this information (whether it is data concerning users or data useful for the correct performance of the services). Data storage on servers is also an element to be taken into consideration, however in this case the information is less interceptable but still vulnerable to threats that can infiltrate the system, such as malware or viruses.
- j. It is very difficult to work with open data to generate applications that use it, and increase its value
- k. Data processing is a major subject. Since the implementation of the GDPR, there is an awareness at the European level
- l. Data breaches that contain sensitive information.

5. Are the training needs for cyber security experts in the transport sector appropriately covered by the existing training curricula? [open-ended]

- a. Seems that improvements are needed
- b. No, a tailored training for security and privacy of transport sector stakeholders is missing.
- c. Partially covered
- d. The cyber security in PT is most probably not really that different from other domains... but it has to be requested and tested.
- e. not fulfilled
- f. Improvements in CS expert curricula to address new incoming cyber threats as well as the new cyber/physical dimension are required
- g. New threats emerging with the Internet-of-Things. It is not evident that this is covered adequately. The minimum requirement is for awareness trainings.
- h. Training on these issues was recently born with the need to have personnel capable of countering cyber-threats. However, there are still few figures with adequate curricula.
- i. no
- j. I don't think transport-related topic is currently the most relevant. But it seems very clear, that it will become so in the near future.
- k. Yes

6. Please provide examples of existing training curricula [open-ended]

- a. National Initiative for Cybersecurity Careers and Studies (US based)
- b. <https://www.k-asap.com/en/>
- c. <https://www.proofpoint.com/us/wombat-security-is-now-proofpoint>
- d. <https://www.knowbe4.com/>
- e. UNI-EN related certification training curricula and specific training on specific product used
- f. IOT cybersecurity courses
- g. In recent years, many universities have launched specific courses in the field of cyber security, both degree and masters' courses.
- h. There are no specific training curricula in cybersecurity and transport
- i. The ENISA best cyber security practices publications.

7. Are you using cybersecurity standards in your work efforts? [multiple choice and open-ended]

- a. No
- b. **Yes: Which of the following areas do these standards cover (System Architecture, System Requirements, Interoperability, Data Handling, Training, other)?**

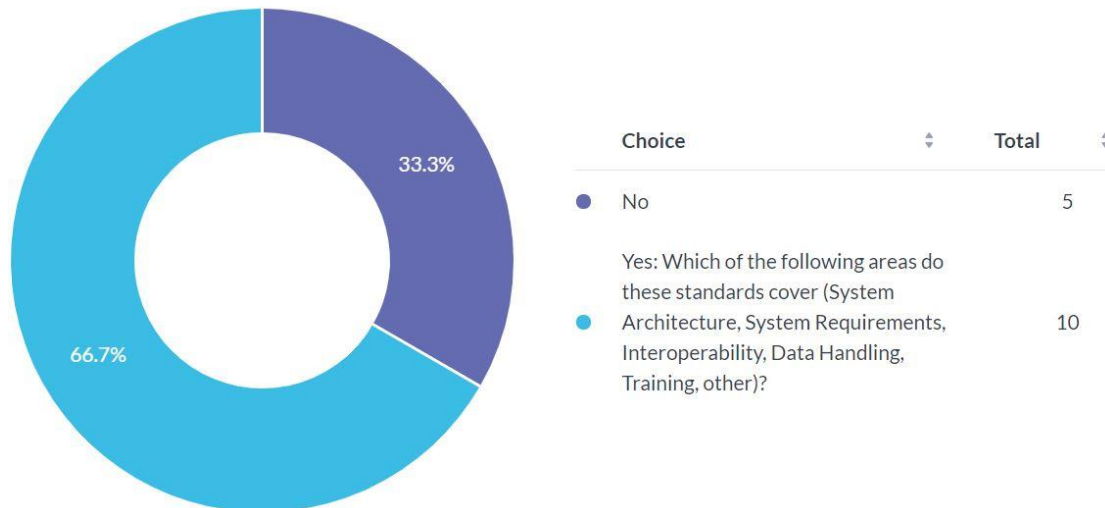


Figure 3: responses to question 7

Areas covered by the used standards:

- Software development
- Data Handling
- system Architecture, Interoperability, data handling
- System Requirements and Interoperability
- System architecture, Interoperability, Data Handling
- Mitre Att&ck
- Infrastructure security, policies for personnel and users, cyber security mechanism, etc.

8. Please name the standards you use the most [open-ended]

- HyperText Markup Language (IETF, ISO, W3C) or HTTP, ECMAScript (ECMA, ISO), JavaScript Object Notation, Structured Query Language (ANSI, ISO) Regarding cybersecurity: ETSI TR 102 893
- ISO/IEC 27001:2013
- HTTPS, SSL, NIST best practise
- Transmodel, NeTEx, SIRI. That's about PT only, without cyber security that is expected to be at a higher level
- ISO/IEC 27001:2013 – Information technology – Security techniques – Information security management systems – Requirements.
- ISO 31000 (<https://www.iso.org/iso-31000-risk-management.html>) and ISO 31010 (<https://www.iso.org/standard/72140.html>) risk management and risk assessment techniques standards.
- Mitre Att&ck
- ISO 27001, ISO 27032

9. Do see any gaps in the current cybersecurity standards in the city transport ecosystem? [multiple choice and open-ended]

- No
- Yes: Which of the following areas do these standards cover (System Architecture, System Requirements, Interoperability, Data Handling, Training, other)?

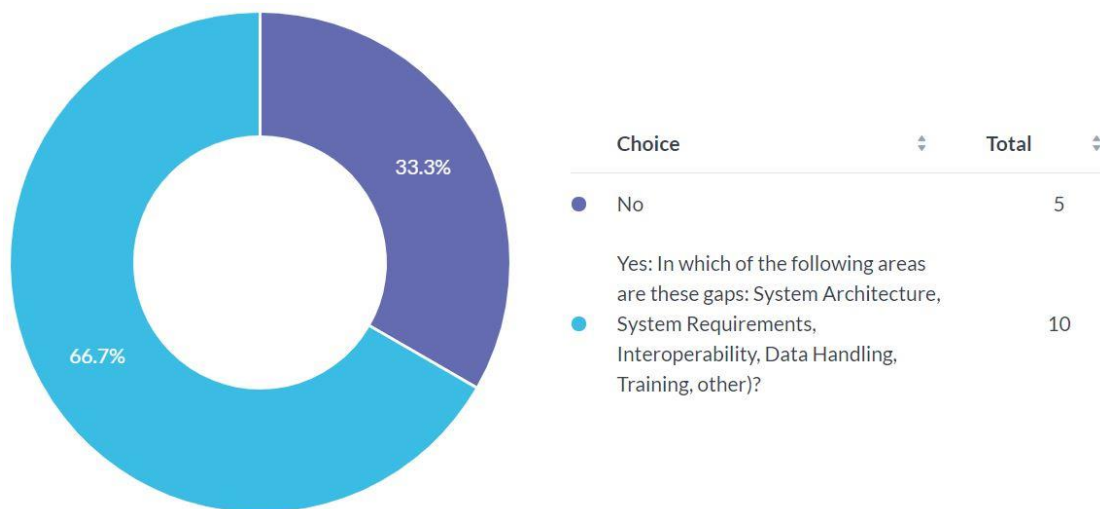


Figure 4: responses to question 9

Areas demonstrating standardization gaps:

- a. Data handling
- b. The cyber security standards gap analysis (<https://cyberwatching.eu/publications/cybersecurity-standard-gap-analysis>) is valid also in the city transport ecosystem
- c. The solutions are there, but first need to be used. Improvement will be a second step
- d. Interoperability
- e. System Architecture and Interoperability
- f. All
- g. Gaps in cybersecurity standards will always exist because threats will continually evolve to exploit every possible vulnerability, so the standards must be periodically updated to ensure optimal efficiency. However, we must always consider the level of application of these standards in the transport ecosystem which is the first problem to be addressed.
- h. All of them

10. Could you name the most urgent standardization gaps? [open-ended]

- a. Cannot prioritize, most likely the most critical direction seems to be the link between data (handling? integrity?) and functional safety
- b. Lack of common language in cyber risk management processes - Lack of integration between Business-Critical processes and cyber security processes
- c. Passenger data handling
- d. real time operational bus data
- e. Current security standards don't cover system architecture definition and interoperability specification.
- f. System Architecture and the lack of widely adopted language and methodology to model the whole transport infrastructure.

- g. There should be an official standard on the standardization of cybersecurity risk linked to multi-modal transport
- h. Data processing and handling between stakeholders.

11. What are your greatest concerns regarding the existing cybersecurity standards? (f.e. which standard to use, usability, coherence between different standards, too generic, complexity of standards, lack of an appropriate standard, other) [open-ended]

- a. Complexity is an issue. The lack of standards in certain areas is also a concern
- b. Once defined, the standard should provide also a set of best practices to make it implementable in an up and running production environment
- c. too many standards available, no general consensus on which standard is to be used
- d. It is a very different domain from the PT domain. PT expert are not fully aware of them. You can't be expert of everything (and PT is already very deep)
- e. which standard to use
- f. (1) Too many generic standards (2) Lack of an appropriate standard
- g. Coherence between different standards, lack of an appropriate standard (ex: to manage social engineering threats)
- h. When it comes to information security, there are several standards. The contents of these standards are often overlaid and cover different fields with different levels of completeness. For example, the NIS directive and ISO27001 deal with the same topic with many aspects in common but also with some differences. Therefore, a single standard may be the optimal solution for companies in order to horizontally refer to the same standards.
- i. Absence of an appropriate standard linked to the multi-modal transport network and the risks that this will generate. The risk of updates (OTA), the dialogue between vehicle (V to V) and between vehicle and road infrastructure (V to I) will create a lot of risk and vulnerability
- j. Certain standards are too generic and high-level.

12. Are your city multimodal systems compliant with transport European data exchange standards (Transmodel, SIRI, NeTEx)? [multiple choice]

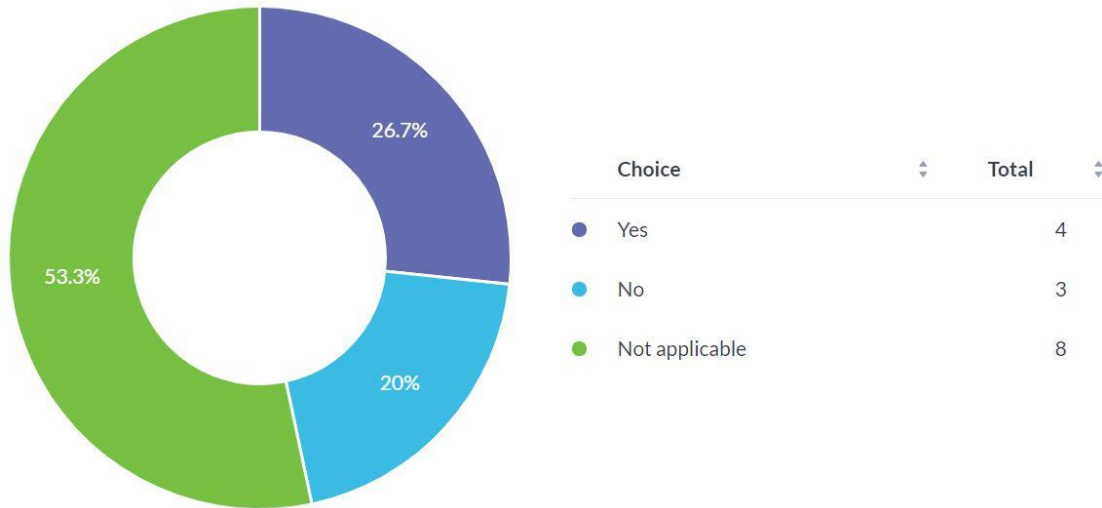


Figure 5: responses to question 12

ANNEX 2: LIST OF IDENTIFIED FORMAL STANDARDS

NOTE – Some Standards (published and under development) and Standardization bodies are hyperlinked to websites for detailed information, incl. previews of standard content.

	Standardization Body	Title	Status	Summary	CitySCAPE Action
1.	CEN/TC 224 , Personal identification and related personal devices with secure element, systems, operations and privacy in a multi-sectorial environment	EN 15320:2007 Identification card systems - Surface transport applications - Interoperable Public Transport Applications - Framework	published	Specifies sets of data presented at an interface, the card sub-system interface, in a structured form as well as the rules for dealing with that data to enable products such as tickets to be written to a Machine Readable Card in a manner which will minimise the amount of data to be held on the card while allowing an authorised party to be able to access and interpret the data easily and efficiently.	
2.	CEN/TC 224 , Personal identification and related personal devices with secure element, systems, operations and privacy in a multi-sectorial environment	EN 1545-2:2015 Identification card systems - Surface transport applications - Part 2: Transport and travel payment related data elements and code lists	published	Specifies data formats, data elements and data elements with associated code lists for use within Surface Transport Applications on ICs.	



This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 883321. Content reflects only the authors' view and European Commission is not responsible for any use that may be made of the information it contains.

	Standardization Body	Title	Status	Summary	CitySCAPE Action
3.	CEN/TC 224 , Personal identification and related personal devices with secure element, systems, operations and privacy in a multi-sectorial environment	CEN/TS 17631 Personal identification - Biometric group access control	published	This document provides guidance on providing access: to areas with physical access control, e.g. entertainment facilities, train stations, shops, libraries, banks, or border control, for small groups of persons, e.g. families with small children or seniors, or other accompanied persons in need of support, by means of biometric authentication technologies, e.g. facial, fingerprint, or vein recognition, in the European regulatory context. The document addresses the following aspects which are specific for biometric and group access: accessibility and usability, user guidance including group guidance and interaction control, privacy including data set content, presentation attack detection, applicable biometric technologies, storage of reference data, biometric process integration, specific needs considering biometrics for groups, biometric performance and error rates, and group internal linkage. The following aspects which reflect on generic access control issues are out of scope: IT security, application specific physical security, policy definition, processes not related to biometric authentication, and specific performance requirements of identification (1:N) and verification (1:1) applications.	
4.	CEN/TC 224 , Personal identification and related personal devices with secure element, systems, operations and privacy in a multi-sectorial environment	CEN/TR 419010 Framework for standardization of signatures - Extended structure including electronic identification and authentication	published	Scope: the document does a brief analysis of the implementing acts on electronic identities CIR 2015/1501 and CIR 2015/1502, and how this is addressed by the eID interoperability framework. It also establishes what areas of existing standards are impacted by the eID framework and what further areas of standardization could assist nations in providing eID services.	

	Standardization Body	Title	Status	Summary	CitySCAPE Action
5.	CEN/TC 224 , Personal identification and related personal devices with secure element, systems, operations and privacy in a multi-sectorial environment	CEN/TS 15480-2:2012 Identification card systems - European Citizen Card - Part 2: Logical data structures and security services	published	Specifies the logical characteristics and security features at the card/system interface for the European Citizen Card.	
6.	CEN/TC 224 , Personal identification and related personal devices with secure element, systems, operations and privacy in a multi-sectorial environment	CEN/TS 15480-4:2012 Identification card systems - European Citizen Card - Part 4: Recommendations for European Citizen Card issuance, operation and use	published	Recommends card issuance and operational procedures including citizens' registration.	
7.	CEN/TC 224 , Personal identification and related personal devices with secure element, systems, operations and privacy in a multi-sectorial environment	CEN/TS 15480-5:2013 Identification card systems - European Citizen Card - Part 5: General Introduction	published	Addresses the difficulties presented to citizens when attempting to access various public services using a smart card as an access token.	

	Standardization Body	Title	Status	Summary	CitySCAPE Action
8.	CEN/TC 224 , Personal identification and related personal devices with secure element, systems, operations and privacy in a multi-sectorial environment	EN 419212-1:2017 Application Interface for Secure Elements for Electronic Identification, Authentication and Trusted Services - Part 1: Introduction and common definitions	published	Provides history, application context, market perspective and a tutorial about the basic understanding of electronic signatures.	
9.	CEN/TC 226 , Road equipment	EN 12675:2017 Traffic signal controllers - Functional safety requirements	published	Specifies the functional safety requirements for traffic signal controllers.	
10.	CEN/TC 226 , Road equipment	EN 16303:2020 Road restraint systems - Validation and verification process for the use of virtual testing in crash testing against vehicle restraint system	published	Defines the accuracy, credibility and confidence in the results of virtual crash test to vehicle restraint systems through the definition of procedures for verification, validation and development of numerical models for roadside safety application. Finally it defines a list of indications to ensure the competences of an expert/organization in the domain of virtual testing. The scope of this document is also applicable to passive safety devices	
11.	CEN/TC 278 , Intelligent transport system	EN 12896-1:2016 Public transport - Reference data model - Part 1: Common concepts	published	Objective of the EN 12896 series of standards: present the Public Transport Reference Data Model based on: - the Public Transport Reference Data Model published 2006 as EN12896 and known as Transmodel V5.1, - the model for the Identification of Fixed Objects for Public transport, published 2009 as EN 28701 and known as IFOPT, incorporating the requirements of - EN15531-1 to 3 and TSI5531-4 and 5: Service interface for real-time information relating to public transport operations (SIRI),- TSI6614-1 and 2: Network and Timetable Exchange (NeTeX), in particular the specific needs for long distance train operation. Particular attention is drawn to the data model structure and methodology.	CSG: This standard is not directly used in CitySCAPE labelling work because it defines a conceptual model. On the other hand, systems implementing SIRI & NeTeX standards, should comply with them as they use the same concepts. Transmodel contributes to the design of scalable and interoperable transport systems Refer to the different parts of the standard (Part 2 to 8)

	Standardization Body	Title	Status	Summary	CitySCAPE Action
12.	CEN/TC 278 , Intelligent transport system	EN 12896-2:2016 Public transport - Reference data model - Part 2: Public transport network	published	Objective of the EN 12896 series of standards: present the Public Transport Reference Data Model based on: - the Public Transport Reference Data Model published 2006 as EN12896 and known as Transmodel V5.1, - the model for the Identification of Fixed Objects for Public transport, published 2009 as EN 28701 and known as IFOPT, incorporating the requirements of - EN15531-1 to 3 and TS15531-4 and 5: Service interface for real-time information relating to public transport operations (SIRI),- TS16614-1 and 2: Network and Timetable Exchange (NeTeX), in particular the specific needs for long distance train operation. Particular attention is drawn to the data model structure and methodology.	CSG: This standard is not directly used in CitySCAPE labelling work because it defines a conceptual model. On the other hand, systems implementing SIRI & NeTeX standards, should comply with them as they use the same concepts. Transmodel contributes to the design of scalable and interoperable transport systems Refer to the different parts of the standard (Part 2 to 8)
13.	CEN/TC 278 , Intelligent transport system	EN 12896-3:2016 Public transport - Reference data model - Part 3: Timing information and vehicle scheduling	published	Objective of the EN 12896 series of standards: present the Public Transport Reference Data Model based on: - the Public Transport Reference Data Model published 2006 as EN12896 and known as Transmodel V5.1, - the model for the Identification of Fixed Objects for Public transport, published 2009 as EN 28701 and known as IFOPT, incorporating the requirements of - EN15531-1 to 3 and TS15531-4 and 5: Service interface for real-time information relating to public transport operations (SIRI),- TS16614-1 and 2: Network and Timetable Exchange (NeTeX), in particular the specific needs for long distance train operation. Particular attention is drawn to the data model structure and methodology.	CSG: This standard is not directly used in CitySCAPE labelling work because it defines a conceptual model. On the other hand, systems implementing SIRI & NeTeX standards, should comply with them as they use the same concepts. Transmodel contributes to the design of scalable and interoperable transport systems Refer to the different parts of the standard (Part 2 to 8)

	Standardization Body	Title	Status	Summary	CitySCAPE Action
14.	CEN/TC 278 , Intelligent transport system	EN 12896-4:2019 Public transport - Reference data model - Part 4: Operations monitoring and control	published	Objective of the EN 12896 series of standards: present the Public Transport Reference Data Model based on: - the Public Transport Reference Data Model published 2006 as EN12896 and known as Transmodel V5.1, - the model for the Identification of Fixed Objects for Public transport, published 2009 as EN 28701 and known as IFOPT, incorporating the requirements of - EN15531-1 to 3 and TS15531-4 and 5: Service interface for real-time information relating to public transport operations (SIRI),- TS16614-1 and 2: Network and Timetable Exchange (NeTeX), in particular the specific needs for long distance train operation. Particular attention is drawn to the data model structure and methodology.	CSG: This standard is not directly used in CitySCAPE labelling work because it defines a conceptual model. On the other hand, systems implementing SIRI & NeTeX standards, should comply with them as they use the same concepts. Transmodel contributes to the design of scalable and interoperable transport systems Refer to the different parts of the standard (Part 2 to 8)
15.	CEN/TC 278 , Intelligent transport system	EN 12896-5:2019 Public transport - Reference data model - Part 5: Fare management	published	Objective of the EN 12896 series of standards: present the Public Transport Reference Data Model based on: - the Public Transport Reference Data Model published 2006 as EN12896 and known as Transmodel V5.1, - the model for the Identification of Fixed Objects for Public transport, published 2009 as EN 28701 and known as IFOPT, incorporating the requirements of - EN15531-1 to 3 and TS15531-4 and 5: Service interface for real-time information relating to public transport operations (SIRI),- TS16614-1 and 2: Network and Timetable Exchange (NeTeX), in particular the specific needs for long distance train operation. Particular attention is drawn to the data model structure and methodology.	CSG: This standard is not directly used in CitySCAPE labelling work because it defines a conceptual model. On the other hand, systems implementing SIRI & NeTeX standards, should comply with them as they use the same concepts. Transmodel contributes to the design of scalable and interoperable transport systems Refer to the different parts of the standard (Part 2 to 8)

	Standardization Body	Title	Status	Summary	CitySCAPE Action
16.	CEN/TC 278 , Intelligent transport system	EN 12896-6:2019 Public transport - Reference data model - Part 6: Passenger information	published	Objective of the EN 12896 series of standards: present the Public Transport Reference Data Model based on: - the Public Transport Reference Data Model published 2006 as EN12896 and known as Transmodel V5.1, - the model for the Identification of Fixed Objects for Public transport, published 2009 as EN 28701 and known as IFOPT, incorporating the requirements of - EN15531-1 to 3 and TS15531-4 and 5: Service interface for real-time information relating to public transport operations (SIRI),- TS16614-1 and 2: Network and Timetable Exchange (NeTeX), in particular the specific needs for long distance train operation. Particular attention is drawn to the data model structure and methodology.	CSG: This standard is not directly used in CitySCAPE labelling work because it defines a conceptual model. On the other hand, systems implementing SIRI & NeTeX standards, should comply with them as they use the same concepts. Transmodel contributes to the design of scalable and interoperable transport systems Refer to the different parts of the standard (Part 2 to 8)
17.	CEN/TC 278 , Intelligent transport system	EN 12896-7:2019 Public transport - Reference data model - Part 7: Driver management	published	Objective of the EN 12896 series of standards: present the Public Transport Reference Data Model based on: - the Public Transport Reference Data Model published 2006 as EN12896 and known as Transmodel V5.1, - the model for the Identification of Fixed Objects for Public transport, published 2009 as EN 28701 and known as IFOPT, incorporating the requirements of - EN15531-1 to 3 and TS15531-4 and 5: Service interface for real-time information relating to public transport operations (SIRI),- TS16614-1 and 2: Network and Timetable Exchange (NeTeX), in particular the specific needs for long distance train operation. Particular attention is drawn to the data model structure and methodology.	CSG: This standard is not directly used in CitySCAPE labelling work because it defines a conceptual model. On the other hand, systems implementing SIRI & NeTeX standards, should comply with them as they use the same concepts. Transmodel contributes to the design of scalable and interoperable transport systems Refer to the different parts of the standard (Part 2 to 8)

	Standardization Body	Title	Status	Summary	CitySCAPE Action
18.	CEN/TC 278 , Intelligent transport system	EN 12896-8:2019 Public transport - Reference data model - Part 8: Management information & statistics	published	Objective of the EN 12896 series of standards: present the Public Transport Reference Data Model based on: - the Public Transport Reference Data Model published 2006 as EN12896 and known as Transmodel V5.1, - the model for the Identification of Fixed Objects for Public transport, published 2009 as EN 28701 and known as IFOPT, incorporating the requirements of - EN15531-1 to 3 and TS15531-4 and 5: Service interface for real-time information relating to public transport operations (SIRI),- TS16614-1 and 2: Network and Timetable Exchange (NeTEx), in particular the specific needs for long distance train operation. Particular attention is drawn to the data model structure and methodology.	CSG: This standard is not directly used in CitySCAPE labelling work because it defines a conceptual model. On the other hand, systems implementing SIRI & NeTEx standards, should comply with them as they use the same concepts. Transmodel contributes to the design of scalable and interoperable transport systems Refer to the different parts of the standard (Part 2 to 8)

	Standardization Body	Title	Status	Summary	CitySCAPE Action
19.	CEN/TC 278 , Intelligent transport system	CEN/TS 16614-1:2020 Public transport - Network and Timetable Exchange (NeTEx) - Part 1: Public transport network topology exchange format	published	<p>1.1 General NeTEx is dedicated to the exchange of scheduled data (network, timetable and fare information). It is based on Transmodel V6 (EN 12896 series) and SIRI (CEN/TS 15531-4/-5 and EN 15531-1/-2/-3) and supports the exchange of information of relevance for passenger information about public transport services and also for running Automated Vehicle Monitoring Systems (AVMS).</p> <p>NOTE Many NeTEx concepts are taken directly from Transmodel; the definitions and explanation of these concepts are extracted directly from the respective standard and reused in NeTEx, sometimes with adaptations in order to fit the NeTEx context. Although the data exchanges targeted by NeTEx are predominantly oriented towards provisioning passenger information systems and AVMS with data from transit scheduling systems, it is not restricted to this purpose and NeTEx can also provide an effective solution to many other use cases for transport data exchange.</p> <p>1.2 Transport modes All mass public transport modes are taken into account by NeTEx, including train, bus, coach, metro, tramway, ferry, and their submodes. It is possible to describe airports and air journeys, but there has not been any specific consideration of any additional requirements that apply specifically to air transport.</p> <p>1.3 Compatibility with existing standards and recommendations Concepts covered in NeTEx that relate in particular to long-distance train travel include; rail operators and related organizations; stations and related equipment; journey coupling and journey parts; train composition and facilities; planned passing times; timetable versions and validity conditions. In the case of long distance train the NeTEx takes into account the requirements formulated by the ERA (European Rail Agency) - TAP/TSI (Telematics Applications for Passenger/ Technical Specification for Interoperability, entered into force on 13 May 2011 as the Commission Regulation (EU) No 454/2011), based on UIC directives. As regards the other exchange protocols, a formal compatibility is ensured with TransXChange (UK), VDV 452 (Germany), NEPTUNE (France), UIC Leaflet, BISON (The Netherlands) and NOPTIS (Nordic Public Transport Interface Standard). The data exchange is possible either through dedicated web services, through data file exchanges, or using the SIRI exchange protocol as described in part 2 of the SIRI documentation.</p>	<p>CSG: NeTEx is included in the study carried out as part of Task 8.2. Its evaluation with regard to cybersecurity threats and in the implementation of a labelling process are integrated into the study.</p> <p>NeTEx is unavoidable (mandatory) within the framework of the European directive 2010/40 Action A. Nevertheless, within the framework of CitySCAPE, particular attention is paid to Part 1 which defines the common mechanisms for the exchange of information (identification of subscriptions, requests, etc.)</p>

	Standardization Body	Title	Status	Summary	CitySCAPE Action
20.	CEN/TC 278, Intelligent transport system	CEN/TS 16614-2:2020 Public transport - Network and Timetable Exchange (NeTEx) - Part 2: Public transport scheduled timetables exchange format	published	<p>1.1 General NeTEx is dedicated to the exchange of scheduled data (network, timetable and fare information) based on Transmodel V5.1 (EN 12986), IFOPT (CEN/TS 28701) and SIRI (CEN/TS 15531-4/5 and EN 15531-1/2/3) and supports information exchange of relevance to public transport services for passenger information and AVMS systems.</p> <p>NOTE Many NeTEx concepts are taken directly from Transmodel and IFOPT; the definitions and explanation of these concepts are extracted directly from the respective standards and reused in NeTEx, sometimes with further adaptations in order to fit the NETEx context. The data exchanges targeted by NeTEx are predominantly oriented towards passenger information and also for data exchange between transit scheduling systems and AVMS (Automated Vehicle Monitoring Systems). However it is not restricted to these purposes, and NeTEx can provide an effective solution to many other use cases for transport exchange.</p> <p>1.2 Transport modes Most public transport modes are taken into account by NeTEx, including train, bus, coach, metro, tram-way, ferry, and their submodes. It is possible to describe airports and air journeys, but there has not been any specific consideration of any additional provisions that apply especially to air transport.</p> <p>1.3 Compatibility with existing standards and recommendations The concepts covered in NeTEx that relate in particular to long-distance train travel include; rail operators and related organizations; stations and related equipment; journey coupling and journey parts; train composition and facilities; planned passing times; timetable versions and validity conditions. In the case of long distance train the NeTEx takes into account the requirements formulated by the ERA (European Rail Agency) – TAP/TSI (Telematics Applications for Passenger/ Technical Specification for Interoperability, entered into force on 13 May 2011 as the Commission Regulation (EU) No 454/2011), based on UIC directives. As regards the other exchange protocols, a formal compatibility is ensured with TransXChange (UK), VDV 452 (Germany), NEPTUNE (France), UIC Leaflet, BISON (Netherlands) and NOPTIS (Nordic Public Transport Interface Standard). The data exchange is possible either through dedicated web services, through data file exchanges, or using the SIRI exchange protocol as described in part 2 of the SIRI documentation.</p>	<p>CSG: NeTEx is included in the study carried out as part of Task 8.2. Its evaluation with regard to cybersecurity threats and in the implementation of a labelling process are integrated into the study.</p> <p>NeTEx is unavoidable (mandatory) within the framework of the European directive 2010/40 Action A. Nevertheless, within the framework of CitySCAPE, particular attention is paid to Part 1 which defines the common mechanisms for the exchange of information (identification of subscriptions, requests, etc.)</p>

21.	CEN/TC 278 , Intelligent transport system	CEN/TS 16614-3:2020 Public transport - Network and Timetable Exchange (NeTEx) - Part 3: Public transport fares exchange format	published	<p>1.1 General NeTEx is dedicated to the exchange of scheduled data (network, timetable and fare information). It is based on Transmodel V5.1 (EN 12986), IFOPT (EN 28701) and SIRI (CEN/TS 15531-4/5 and EN 15531-1/2/3) and supports the exchange of information of relevance for passenger information about public transport services and also for running Automated Vehicle Monitoring Systems (AVMS).</p> <p>NOTE NeTEx is a refinement and an implementation of Transmodel and IFOPT; the definitions and explanations of these concepts are extracted directly from the respective standard and reused in NeTEx, sometimes with adaptations in order to fit the NeTEx context. Although the data exchanges targeted by NeTEx are predominantly oriented towards provisioning passenger information systems and AVMS with data from transit scheduling systems, it is not restricted to this purpose and NeTEx can also provide an effective solution to many other use cases for transport data exchange.</p> <p>1.2 Fares scope This Part3 of NeTEx, is specifically concerned with the exchange of fare structures and fare data, using data models that relate to the underlying network and timetable models defined in Part1 and Part2 and the Fare Collection data model defined in Transmodel V5.1. See the use cases below for the overall scope of Part3. In summary, it is concerned with data for the following purposes: (i) To describe the many various possible fare structures that arise in public transport (for example, flat fares, zonal fares, time dependent fares, distance-based fares, stage fares, pay as you go fares, season passes, etc., etc.). (ii) To describe the fare products that may be purchased having these fare structures and to describe the conditions that may attach to particular fares, for example if restricted to specific groups of users, or subject to temporal restrictions. These conditions may be complex. (i) To allow actual price data to be exchanged. Note however that NeTEx does not itself specify pricing algorithms or how fares should be calculated. This is the concern of Fare Management Systems. It may be used may be used to exchange various parameters required for pricing calculations that are needed to explain or justify a fare. (iii) To include the attributes and the text descriptions necessary to present fares and their conditions of sale and use to the public. NeTEx should be regarded as being 'upstream' of retail systems and allows fare data to be managed and integrated with journey planning and network data in public facing information systems. It is complementary to and</p>	<p>CSG: NeTEx is included in the study carried out as part of Task 8.2. Its evaluation with regard to cybersecurity threats and in the implementation of a labelling process are integrated into the study.</p> <p>NeTEx is unavoidable (mandatory) within the framework of the European directive 2010/40 Action A. Nevertheless, within the framework of CitySCAPE, particular attention is paid to Part 1 which defines the common mechanisms for the exchange of information (identification of subscriptions, requests, etc.)</p>
-----	--	---	-----------	--	--

	Standardization Body	Title	Status	Summary	CitySCAPE Action
				<p>distinct from the 'downstream' ticketing and retail systems that sell fares and of the control systems that validate their use. See 'Excluded Use Cases' below for further information on the boundaries of NeTEx with Fare Management Systems.</p> <p>1.3 Transport modes All mass public transport modes are taken into account by NeTEx, including train, bus, coach, metro, tramway, ferry, and their submodes. It is possible to describe airports, air journeys, and air fares, but there has not been any specific consideration of any additional requirements that apply specifically to air transport.</p>	
22.	CEN/TC 278 , Intelligent transport system	CEN/TS 16614-4:2020 Public transport - Network and Timetable Exchange (NeTEx) - Part 4: Passenger Information European Profile	published	<p>This technical specification is a profile of CEN/TS 16614 series. It focuses on information relevant to feed passenger information services and excludes operational and fares information. NeTEx is dedicated to the exchange of scheduled data (network, timetable and fare information) based on Transmodel V6 (EN 12986) and SIRI (CEN/TS 15531-4/5 and EN 15531-1/2/3) and supports information exchange of relevance to public transport services for passenger information and AVMS systems. As for most data exchange standards, defining subsets of data and dedicated rules for some specific use case is of great help for implementers and for the overall interoperability. This subset is usually called profile and this profile targets passenger information as only use case.</p>	<p>CSG: NeTEx is included in the study carried out as part of Task 8.2. Its evaluation with regard to cybersecurity threats and in the implementation of a labelling process are integrated into the study.</p> <p>NeTEx is unavoidable (mandatory) within the framework of the European directive 2010/40 Action A. Nevertheless, within the framework of CitySCAPE, particular attention is paid to Part 1 which defines the common mechanisms for the exchange of information (identification of subscriptions, requests, etc.)</p>

	Standardization Body	Title	Status	Summary	CitySCAPE Action
23.	CEN/TC 278 , Intelligent transport system	EN 16157-1:2018 Intelligent transport systems - DATEX II data exchange specifications for traffic management and information - Part 1: Context and framework	published	<p>This document specifies and defines components required to support the exchange and shared use of data and information in the field of traffic and travel. The components include the framework and context for the modelling approach, data content, data structure and relationships. This document is applicable to:</p> <ul style="list-style-type: none"> - traffic and travel information which is of relevance to road networks (non-urban and urban), - public transport information that is of direct relevance to the use of a road network (e.g. road link via train or ferry service), - traffic and travel information in the case of Cooperative intelligent transport systems (C-ITS). <p>This document establishes specifications for data exchange between any two instances of the following actors:</p> <ul style="list-style-type: none"> - Traffic Information Centres (TICs), - Traffic Control Centres (TCCs), - Service Providers (SPs), <p>Use of this document can be applicable for use by other actors. This document covers, at least, the following types of informational content:</p> <ul style="list-style-type: none"> - road traffic event information - planned and unplanned occurrences both on the road network and in the surrounding environment, - information about operator-initiated actions - including both advisory and mandatory measures, - road traffic measurement data, status data, and travel time data, - travel information relevant to road users, including weather and environmental information, - road traffic management information and information and advice relating to use of the road network. <p>This part of EN 16157 specifies the DATEX II framework of all parts of this European Standard, the context of use and the modelling approach taken and used throughout this European Standard. This approach is described using formal methods and provides the mandatory reference framework for all other parts.</p>	<p>CSG: DATEXII is a standard centred on road traffic which does not fall directly within the scope of task 8.2. However, the information it conveys may relate to transport systems (route search). The services provided by this standard will be considered in task T8.2</p>

	Standardization Body	Title	Status	Summary	CitySCAPE Action
24.	CEN/TC 278 , Intelligent transport system	EN 16157-2:2019 Intelligent transport systems - DATEX II data exchange specifications for traffic management and information - Part 2: Location referencing	published	<p>This European Standard series (EN 16157) specifies and defines component facets supporting the exchange and shared use of data and information in the field of traffic and travel. The component facets include the framework and context for exchanges, the modelling approach, data content, data structure and relationships. This European Standard series is applicable to:</p> <ul style="list-style-type: none"> - traffic and travel information which is of relevance to road networks (non-urban and urban), - public transport information that is of direct relevance to the use of a road network (e.g. road link via train or ferry service), - traffic and travel information in the case of Cooperative intelligent transport systems (C-ITS). <p>This European Standard series establishes specifications for data exchange between any two instances of the following actors:</p> <ul style="list-style-type: none"> - Traffic Information Centres (TICs), - Traffic Control Centres (TCCs), - Service Providers (SPs). <p>Use of this European Standard series may be applicable for use by other actors. This European Standard series covers, at least, the following types of informational content:</p> <ul style="list-style-type: none"> - road traffic event information – planned and unplanned occurrences both on the road network and in the surrounding environment, - operator initiated actions, - road traffic measurement data, status data, and travel time data, - travel information relevant to road users, including weather and environmental information, - road traffic management information and instructions relating to use of the road network. <p>This part of the EN 16157 series specifies the informational structures, relationships, roles, attributes and associated data types, for the implementation of the location referencing systems used in association with the different publications defined in the Datex II framework. It also defines a DATEX II publication for exchanging predefined locations. This is part of the DATEX II platform independent data model.</p>	<p>CSG: DATEXII is a standard centred on road traffic which does not fall directly within the scope of task 8.2. However, the information it conveys may relate to transport systems (route search). The services provided by this standard will be considered in task T8.2</p>

	Standardization Body	Title	Status	Summary	CitySCAPE Action
25.	CEN/TC 278 , Intelligent transport system	EN 16157-3:2018 Intelligent transport systems - DATEX II data exchange specifications for traffic management and information - Part 3: Situation Publication	published	<p>This document specifies and defines component facets supporting the exchange and shared use of data and information in the field of traffic and travel. The component facets include the framework and context for exchanges, the modelling approach, data content, data structure and relationships. This document is applicable to:</p> <ul style="list-style-type: none"> - traffic and travel information which is of relevance to road networks (non-urban and urban), - public transport information that is of direct relevance to the use of a road network (e.g. road link via train or ferry service), - traffic and travel information in the case of Cooperative intelligent transport systems (C-ITS). <p>This document establishes specifications for data exchange between any two instances of the following actors:</p> <ul style="list-style-type: none"> - Traffic Information Centres (TICs), - Traffic Control Centres (TCCs), - Service Providers (SPs), <p>Use of this document can be applicable for use by other actors. This document covers, at least, the following types of informational content:</p> <ul style="list-style-type: none"> - road traffic event information - planned and unplanned occurrences both on the road network and in the surrounding environment, - operator-initiated actions, - road traffic measurement data, status data, and travel time data, - travel information relevant to road users, including weather and environmental information, - road traffic management information and instructions relating to use of the road network. <p>This document specifies the informational structures, relationships, roles, attributes and associated data types required for publishing situation traffic and travel information within the DATEX II framework. This is specified as a DATEX II Situation Publication sub-model which is part of the DATEX II platform independent model, but this part excludes those elements that relate to:</p> <ul style="list-style-type: none"> - location information which are specified in FprEN 16157 2; - common information elements, which are specified in EN 16157 7. 	<p>CSG: DATEXII is a standard centred on road traffic which does not fall directly within the scope of task 8.2. However, the information it conveys may relate to transport systems (route search). The services provided by this standard will be considered in task T8.2</p>

26.	CEN/TC 278 , Intelligent transport system	EN 16157-4:2021 Intelligent transport systems - DATEX II data exchange specifications for traffic management and information - Part 4: Variable Message Sign (VMS) Publications	published	<p>This European Standard (EN 16157 series) specifies and defines component facets supporting the exchange and shared use of data and information in the field of traffic and travel. The component facets include the framework and context for exchanges, the modelling approach, data content, data structure and relationships. This European Standard is applicable to:</p> <ul style="list-style-type: none"> - Traffic and travel information which is of relevance to road networks (non-urban and urban), - Public transport information that is of direct relevance to the use of a road network (e.g. road link via train or ferry service), - Traffic and travel information in the case of Cooperative intelligent transport systems (C-ITS). <p>This European Standard establishes specifications for data exchange between any two instances of the following actors:</p> <ul style="list-style-type: none"> - Traffic Information Centres (TICs), - Traffic Control Centres (TCCs), - Service Providers (SPs), <p>Use of this European Standard may be applicable for use by other actors. This European Standard series covers, at least, the following types of informational content:</p> <ul style="list-style-type: none"> - Road traffic event information – planned and unplanned occurrences both on the road network and in the surrounding environment, - Operator initiated actions, - Road traffic measurement data, status data, and travel time data, - Travel information relevant to road users, including weather and environmental information, - Road traffic management information and instructions relating to use of the road network. <p>This part of the CEN/TS 16157 series specifies the informational structures, relationships, roles, attributes and associated data types required for publishing variable message sign information within the Datex II framework. This is specified in two publications, a DATEX II VMS Table Publication sub-model and a VMS Publication sub-model, which are part of the DATEX II platform independent model, but this part excludes those elements that relate to:</p> <ul style="list-style-type: none"> - location information which are specified in EN 16157-2, - common information elements, which are specified in EN 16157-7, - situation information which are specified in EN 16157-3. 	<p>CSG: DATEXII is a standard centred on road traffic which does not fall directly within the scope of task 8.2. However, the information it conveys may relate to transport systems (route search). The services provided by this standard will be considered in task T8.2</p>
-----	--	---	-----------	---	---

	Standardization Body	Title	Status	Summary	CitySCAPE Action
				<p>The VMS Table Publication supports the occasional exchange of tables containing generally static reference information about deployed VMS which enable subsequent efficient references to be made to pre-defined static information relating to those VMS. The VMS Publication supports the exchange of the graphic and textual content of one or several VMS plus any status information on device configuration that aid the comprehension of the informational content. This content is potentially subject to rapid change. These publications are not intended to support the control or configuration of VMS equipment. Each is part of the DATEX II platform independent model.</p>	

	Standardization Body	Title	Status	Summary	CitySCAPE Action
27.	CEN/TC 278 , Intelligent transport system	EN 16157-7:2018 Intelligent transport systems - DATEX II data exchange specifications for traffic management and information - Part 7: Common data elements	published	<p>This document specifies and defines component facets required to support the exchange and shared use of data and information in the field of traffic and travel. The component facets include the framework and context for data content, data structure and relationships, communications specification. This document is applicable to:</p> <ul style="list-style-type: none"> - traffic and travel information which is of relevance to road networks (non-urban and urban), - public transport information that is of direct relevance to the use of a road network (e.g. road link via train or ferry service), - traffic and travel information in the case of Cooperative intelligent transport systems (C-ITS). <p>This document establishes specifications for data exchange between any two instances of the following actors:</p> <ul style="list-style-type: none"> - Traffic Information Centres (TICs), - Traffic Control Centres (TCCs), - Service Providers (SPs), <p>Use of this document can be applicable for use by other actors. This document covers, at least, the following types of informational content:</p> <ul style="list-style-type: none"> - road traffic event information - planned and unplanned occurrences both on the road network and in the surrounding environment, - information about operator initiated actions - including both advisory and mandatory measures, - road traffic measurement data, status data, and travel time data, - travel information relevant to road users, including weather and environmental information, - road traffic management information and information and advice relating to use of the road network. <p>This part of EN 16157 specifies common informational structures, relationships, roles, attributes and associated data types required for publishing information within the DATEX II framework. This is specified as a DATEX II sub-model which is part of the DATEX II platform independent model, but this part only covers common elements that are used by more than one publication. It excludes those elements that relate to location information which are specified in FprEN 16157 2.</p>	<p>CSG: DATEXII is a standard centred on road traffic which does not fall directly within the scope of task 8.2. However, the information it conveys may relate to transport systems (route search). The services provided by this standard will be considered in task T8.2</p>

	Standardization Body	Title	Status	Summary	CitySCAPE Action
28.	CEN/TC 278 , Intelligent transport system	CEN/TS 16157-8:2020 Intelligent transport systems - DATEX II data exchange specifications for traffic management and information - Part 8: Traffic management publications and extensions dedicated to the urban environment	published	<p>This document constitutes a Part of the CEN 16157 DATEX II series of standards and technical specifications. This series specifies and defines component facets supporting the exchange and shared use of data and information in the field of traffic and travel. The component facets include the framework and context for exchanges, the modelling approach, the data content, the data structure and relationships and the communications specification. Part 8, this document, specifies additional data model structures that are applicable for traffic management applications in the urban environment. This Part addresses data concepts to support the exchange of Traffic Management Plans, rerouting, extensions of the existing DATEX II core model to better support application to the urban environment. It establishes specifications for data exchange between any two instances of the following actors:</p> <ul style="list-style-type: none"> - Traffic Information Centres (TICs), - Traffic Control Centres (TCCs), - Service Providers (SPs). <p>Use of this document may be applicable for use by other actors.</p>	<p>CSG: DATEXII is a standard centred on road traffic which does not fall directly within the scope of task 8.2. However, the information it conveys may relate to transport systems (route search). The services provided by this standard will be considered in task T8.2</p>
29.	CEN/TC 278 , Intelligent transport system	CEN/TS 16157-9:2020 Intelligent transport systems - DATEX II data exchange specifications for traffic management and information - Part 9: Traffic signal management publications dedicated to the urban environment	published	<p>This document constitutes a part of the CEN 16157 DATEX II series of standards and technical specifications. This series specifies and defines component facets supporting the exchange and shared use of data and information in the field of traffic and travel. The component facets include the framework and context for exchanges, the modelling approach, the data content, the data structure and relationships and the communications specification. Part 9, this document, specifies additional data model structures that are applicable for traffic signal management applications in the urban environment. This part specifies data concepts to support the exchange of traffic signal status messaging, intersection geometry definition and attribution in a consistent way with existing C-ITS standards and technical specifications. It establishes specifications for data exchange between any two instances of the following actors:</p> <ul style="list-style-type: none"> - Traffic Information Centres (TICs), - Traffic Control Centres (TCCs), - Service Providers (SPs). <p>Use of this document may be applicable for use by other actors.</p>	<p>CSG: DATEXII is a standard centred on road traffic which does not fall directly within the scope of task 8.2. However, the information it conveys may relate to transport systems (route search). The services provided by this standard will be considered in task T8.2</p>

30.	CEN/TC 278, Intelligent transport system	EN 15531-1:2015 Public transport - Service interface for real-time information relating to public transport operations –Part 1 : Context and Framework	published	<p>1.1 Interfaces specified by this standard</p> <p>1.1.1 Business context Real-time information may be exchanged between a number of different organizations, or between different systems belonging to the same organization. Key interfaces include the following:</p> <ul style="list-style-type: none"> - Between public transport vehicle control centres – generally, for fleet and network management. - Between a control centre and an information provision system – generally, to provide operational information for presentation to the public. - Between information provision systems – generally, sharing information to ensure that publicly available information is complete and comprehensive. - Between information provision systems – and data aggregation systems that collect and integrate data from many different sources and different types of data supplier and then distribute it onwards. - Between information provision systems and passenger information devices such as mobile phones, web browsers, etc. <p>Annex B describes the business context for SIRI in more detail. SIRI is intended for wide scale, distributed deployment by a wide variety of installations. In such circumstances it is often not practical to upgrade all the systems at the same time. SIRI therefore includes a formal versioning system that allows for the concurrent operation of different levels at the same time and a disciplined upgrade process. In this general framework, SIRI defines a specific set of concrete functional services. The services separate the communication protocols from the message content ('functional services'). This allows the same functional content to be exchanged using different transport mechanisms, and different patterns of exchange. Figure 1 below shows this diagrammatically.</p> <p>1.1.2 SIRI communications SIRI provides a coherent set of functional services for exchanging data for different aspects of PT operation. A common data model, based on Transmodel 5.1, is used across all services. A communication layer defines common procedures for the requesting and exchanging of data. Within SIRI, the same general communication protocols are used for all the different concrete functional interfaces, and specify a common infrastructure for message referencing, error handling, reset behaviour and so forth. The communications layer is defined in Part 2 of the SIRI document set. To allow the most efficient use to be made of bandwidth and processing capacity, the SIRI communications architecture supports several different patterns of interaction. SIRI supports both request/response and publish/subscribe protocols between servers, allowing applications both to pull or to push data. The SIRI</p>	CSG: SIRI is integrated into the study carried out as part of task T8.2. Generic mechanisms will be integrated into this analysis.
-----	--	--	-----------	--	--

	Standardization Body	Title	Status	Summary	CitySCAPE Action
				<p>publish/subscribe pattern of interaction follows the paradigm described in the W3C candidate standard 'Publish-Subscribe Notification for Web Services (WS-PubSub)'. SIRI uses the same separation of concerns, and a similar terminology for Publish/Subscribe concepts as is used in WS-PubSub. For the delivery of data in response to both requests and subscriptions, SIRI supports two common patterns of message exchange as realised in existent national systems: - one-step 'direct' delivery: allowing the simple rapid delivery of data; - two-step 'fetched' delivery: allowing a more optimised use of limited resources. 1.1.3 SIRI functional services SIRI provides specific protocols for the following functional services, defined in Part 3 of the SIRI document set: - Production Timetable (PT) Service: to send daily information on the operational timetable and associated vehicle running information. - Estimated Timetable (ET) Service: to send real-time information on timetable, including changes based on the production service and on actual running conditions. - Stop Timetable (ST) Service: to provide a stop-centric view of timetabled vehicle arrivals and departures at a designated stop. - Stop Monitoring (SM) Service: to send real-time arrival & departure information relating to a specific stop.</p>	

31.	CEN/TC 278 , Intelligent transport system	EN 15531-2:2015 Public transport - Service interface for real-time information relating to public transport operations - Part 2: Communications infrastructure	published	<p>SIRI uses a consistent set of general communication protocols to exchange information between client and server. The same pattern of message exchange may be used to implement different specific functional interfaces as sets of concrete message content types. Two well-known specific patterns of client server interaction are used for data exchange in SIRI: Request/Response and Publish/Subscribe. — Request/Response allows for the ad hoc exchange of data on demand from the client. — Publish/Subscribe allows for the repeated asynchronous push of notifications and data to distribute events and Situations detected by a Real-time Service. The use of the Publish/Subscribe pattern of interaction follows that described in the Publish-Subscribe Notification for Web Services (WS-PubSub) specification, and as far as possible, SIRI uses the same separation of concerns and common terminology for publish/subscribe concepts and interfaces as used in WS-PubSub. WS-PubSub breaks down the server part of the Publish/Subscribe pattern into a number of separate named roles and interfaces (for example, Subscriber, Publisher, Notification Producer, and Notification Consumer): in an actual SIRI implementation, certain of these distinct interfaces may be combined and provided by a single entity. Although SIRI is not currently implemented as a full WS-PubSub web service, the use of a WS-PubSub architecture makes this straightforward to do in future. Publish/Subscribe will not normally be used to support large numbers of end user devices. For the delivery of data in responses (to both requests and subscriptions), SIRI supports two common patterns of message exchange, as realised in existent national systems: — A one step ‘Direct Delivery’, as per the classic client-server paradigm, and normal WS-PubSub publish subscribe usage; and; — A two-step ‘Fetched Delivery’ which elaborates the delivery of messages into a sequence of successive messages pairs to first notify the client, and then to send the data when the client is ready. Fetched Delivery is a stateful pattern in its own right. Each delivery pattern allows different trade-offs for implementation efficiency to be made as appropriate for different target environments. A SIRI implementation may support either or both delivery methods; in order to make the most efficient use of the available computational and communication resources. The delivery method may either be preconfigured and static for a given implementation, or each request or subscription may indicate the delivery method required by the client dynamically as part of the request policy, and the server may refuse a request if it does not</p>	<p>CSG: SIRI is integrated into the study carried out as part of task T8.2. Generic mechanisms will be integrated into this analysis.</p>
-----	--	--	-----------	---	---

	Standardization Body	Title	Status	Summary	CitySCAPE Action
				<p>support that method, giving an appropriate error code. The Interaction patterns and the Delivery patterns are independent aspects of the SIRI protocol and may be used in any combination in different implementations. For a given SIRI Functional Service type (Connection Monitoring, Stop Monitoring etc.), the message payload content is the same regardless of whether information is exchanged with a Request/Response or Publish/Subscribe pattern, or whether it is returned by Direct or Fetched Delivery. The SIRI Publish/Subscribe Protocol prescribes particular mediation behaviour for reducing the number of notifications and the amount of network traffic arising from subscriptions. The mediation groups the various subscriptions from a subscriber into one or more Subscriber Channels, and is able to manage notifications and updates for the aggregate. Only partial updates to the data set since the last delivery for the subscription need to be sent. The SIRI Communication protocols are designed to fail gracefully. Considerations for resilience and recovery are covered below.</p>	

32.	CEN/TC 278 , Intelligent transport system	EN 15531-3:2015 Public transport - Service interface for real-time information relating to public transport operations - Part 3: Functional service interfaces	published	<p>There are many potential ways for passenger transport operations centres to interact. The approach taken by SIRI is for an open-ended set of standard data structures, carried over a communications channel constructed using one of a small number of specific options. Part 2 of this European Standard specifies the communications channel. Part 3 specifies a number of functional modules, based on the 'use cases' identified in Annex B to Part 1: — Production Timetable (PT): this service enables the provision of information on the planned progress of vehicles operating a specific service, identified by the vehicle time of arrival and departure at specific stops on a planned route for a particular Operational Day. — Estimated Timetable (ET): this service enables the provision of information on the actual progress of Vehicle Journeys operating specific service lines, detailing expected arrival and departure times at specific stops on a planned route. There will be recorded data for stops which have been passed, and predicted data for stops not yet passed. In addition the Estimated Timetable service allows Vehicle Journeys to be cancelled, added or changed. — Stop Timetable (ST): this service provides a stop-centric view of timetabled vehicle arrivals and departures at a designated stop. It can be used to reduce the amount of information that needs to be transmitted in real-time to stops and displays, as reference data for a Stop Monitoring Service; and provides a data feed of the static timetables. — Stop Monitoring (SM): this service provides a stop-centric view of vehicle arrivals and departures at a designated stop. It can be used by displays and other presentation services to provide departure board and other presentations of timetable and real-time journey information both at stops and at a distance. — Vehicle Monitoring (VM): this service enables the provision of information on the current location and status of a set of vehicles. It provides all the current relevant information from one AVMS relating to all vehicles fulfilling a set of selection criteria. — Connection Timetable (CT): this service may be used to provide information about the scheduled arrivals of a feeder vehicle to the operator of a connecting distributor service. The distributor operator can then plan how to guarantee the connection, either with the expected vehicle or a different vehicle. — Connection Monitoring (CM): this service is used to provide information about the expected arrival of a feeder vehicle to the operator of a connecting distributor service. The distributor operator can then manage the service to guarantee the connection, based on actual vehicle running. — General Message (GM): the SIRI "General</p>	<p>CSG: SIRI is integrated into the study carried out as part of task T8.2. Generic mechanisms will be integrated into this analysis.</p>
-----	--	--	-----------	---	---

	Standardization Body	Title	Status	Summary	CitySCAPE Action
				Message” service is used to exchange informative messages between identified individuals in free or an arbitrary structured format. It enables messages to be sent and to be revoked. Messages are assigned validity periods in addition to the actual content.	
33.	CEN/TC 278 , Intelligent transport system	CEN/TS 15531-4:2021 Public transport - Service interface for real-time information relating to public transport operations - Part 4: Functional service interfaces: Facility monitoring	Published	This document specifies an additional SIRI functional service to exchange information about changes to availability of facilities, between monitoring systems and servers containing real-time public transport vehicle or journey time data. These include the control centres of transport operators, as well as information systems that deliver passenger travel information services. As for Transmodel, public transport modes include new modes of transport (vehicle sharing, vehicle pooling, etc.). This document describes the SIRI Facility Monitoring service, one of a modular set of services for the exchange of Real-time information. The Facility Monitoring service (SIRI-FM) is concerned with the exchange of information about alterations to the availability of facilities for passengers among systems, including equipment monitoring, real-time management and dissemination systems.	CSG: SIRI is integrated into the study carried out as part of task T8.2. Generic mechanisms will be integrated into this analysis.
34.	CEN/TC 278 , Intelligent transport system	CEN/TS 15531-5:2016 Public transport - Service interface for real-time information relating to public transport operations - Part 5: Functional service interfaces: Situation exchange	Published	The scope of this WI is to update CEN/TS 15531-5:2011 which describes structured incident model for disruptions to services, in terms that relate directly to the entities of other SIRI services. Incidents can then be directly linked to stops, lines, journeys, etc in two ways: as the cause of disruption or as the result of service problems. The Incident Monitoring Service is capable of filtering on incident, service and location model attributes. First implementations of the Situation Exchange Service have revealed a number of improvements and some minor enhancements necessary for a successful and uniform usage of the specification in the future. The main elements out of this work item will be: <ul style="list-style-type: none"> o Prepare an updated edition of the TS as a document o Update the common XSD of SIRI parts 1-5 The new work item will consider the work of <ul style="list-style-type: none"> o PT companies and IT-suppliers in Germany o PT companies and IT-suppliers in France o PT companies and IT-suppliers in Sweden using Situation Exchange Service in their projects. 	CSG: SIRI is integrated into the study carried out as part of task T8.2. Generic mechanisms will be integrated into this analysis.

	Standardization Body	Title	Status	Summary	CitySCAPE Action
35.	CEN/TC 278 , Intelligent transport system	CEN/TS 16794-1:2019 Public transport - Communication between contactless readers and fare media - Part 1: Implementation requirements for ISO/IEC 14443	published	This document constitutes the 3rd edition of CEN/TS 16794-1. It sets out the technical requirements to be met by contactless Public Transport (PT) devices in order to be able to interface together using the ISO/IEC 14443 series contactless communications protocol. This document applies to PT devices: - PT readers which are contactless fare management system terminals acting as a PCD contactless reader based on the ISO/IEC 14443 series; - PT objects which are contactless fare media acting as a PICC contactless object based on the ISO/IEC 14443 series. This edition addresses interoperability of consumer-market NFC mobile devices, compliant to NFC Forum specifications, with above mentioned PT devices, aligns with the 4th edition of the ISO/IEC 14443 series and maintains the possibility for PT readers to comply with the requirements from EMV Contactless Interface Specification [1] and the present document. An interface-oriented test approach is used to evaluate the conformity of PT devices and is defined in CEN/TS 16794-2. Application-to-application exchanges executed once contactless communication has been established at RF level fall outside the scope of this document. In line with the rules on independence between OSI protocol layers, this document works on the assumption that application-to-application exchanges are not contingent on the type of contactless communication established or the parameters used for the low-level protocol layers that serve as the platform for these application-to-application exchanges.	

	Standardization Body	Title	Status	Summary	CitySCAPE Action
36.	CEN/TC 278 , Intelligent transport system	CEN/TS 16794-2:2019 Public transport - Communication between contactless readers and fare media - Part 2: Test plan for ISO/IEC 14443	published	<p>This document comes as a complement to the technical requirements expressed in CEN/TS 16794 1, for ensuring contactless communication interoperability between Public Transport (PT) devices or between PT devices compliant to CEN/TS 16794-1 and NFC mobiles devices compliant to NFC Forum specifications. This document lists all the test conditions to be performed on a PT reader or a PT object in order to ensure that all the requirements specified in CEN/TS 16794 1 are met for the PT device under test. This document applies to PT devices only: - PT readers which are contactless fare management system terminals acting as a PCD contactless reader based on the ISO/IEC 14443 series; - PT objects which are contactless fare media acting as a PICC contactless object based on the ISO/IEC 14443 series. This document applies solely to the contactless communication layers described in Parts 1 to 4 of the ISO/IEC 14443 series. Application-to-application exchanges executed once contactless communication has been established at RF level fall outside the scope of this document. However, a test application will be used so as to make end-to-end transactions during tests on the RF communication layer. This document does not duplicate the contents of the ISO/IEC 14443 series or ISO/IEC DIS 10373-6 standard. It makes reference to the ISO/IEC DIS 10373 6 applicable test methods, specifies the test conditions to be used and describes the additional specific test conditions that may be run. The list of test conditions applicable to the PT device under test will be conditioned by the Information Conformance Statement (ICS) declaration made by the device manufacturer. For each test case, the test conditions are clearly specified in order to determine the pertinence to run or not the test case in accordance with the device capabilities or in accordance with the device manufacturer's choice. In order to facilitate the test report issuance, a test report template is included in Annex A of this document. Although this document aims at becoming the primary basis for certification of contactless communication protocol applicable to PT readers and PT objects, it does not describe any certification or qualification processes as such processes should be defined between local or global transit industry stakeholders.</p>	

	Standardization Body	Title	Status	Summary	CitySCAPE Action
37.	CEN/TC 278 , Intelligent transport system	CEN ISO/TS 21177:2019 Intelligent transport systems - ITS station security services for secure session establishment and authentication between trusted devices (ISO/TS 21177:2019)	published	it contains specifications for a set of ITS station security services required to ensure the authenticity of the source and integrity of information exchanged between trusted entities: — devices operated as bounded secured managed entities, i.e. "ITS Station Communication Units" (ITS-SCU) and "ITS station units" (ITS-SU) specified in ISO 21217, and — between ITS-SUs (composed of one or several ITS-SCUs) and external trusted entities such as sensor and control networks. These services include authentication and secure session establishment which are required to exchange information in a trusted and secure manner. These services are essential for many ITS applications and services including time-critical safety applications, automated driving, remote management of ITS stations (ISO 24102-2), and roadside/infrastructure related services.	
38.	CEN Workshop CIRRUS	CWA 16871-1:2015-03-25 Requirements and Recommendations for Assurance in Cloud Security. Contributed recommendations from European projects	published	CWA Recommendations for Assurance in Cloud Security (RACS) promotes recommendations on security assurance management in the context of auditing and certification of cloud-based services and systems. The recommendations in the present document have been collected from a number of EU research pioneer projects in cloud assurance and from RACS target different stakeholders (policy makers, industry and final users) interested in upcoming challenges concerning cloud security assurance. The focus of CWA RACS is mainly on the type of assurance and assessment activities that can be done without the physical presence of an auditor and at any point in time.	
39.	CLC/TC 9X Electrical and electronic applications for railways	CLC/FprTS 50701 Railway applications - Cybersecurity	published	Provides railway operators, system integrators and product suppliers with guidance and specifications on how cybersecurity will be managed in the context of the EN 50126-1 RAMS lifecycle process.	
40.	CLC/TC 9X Electrical and electronic applications for railways	EN 62290-2:2014 Railway applications - Urban guided transport management and command/control systems - Part 2: Functional requirements specification	published	Specifies the functional requirements of UGTMSs (Urban Guided Transport Management and Command/Control Systems) for use in urban guided passenger transport lines and networks.	

	Standardization Body	Title	Status	Summary	CitySCAPE Action
41.	CLC/TC 9X Electrical and electronic applications for railways	EN IEC 62290-3:2019 Railway applications - Urban guided transport management and command/control systems - Part 3: System requirements specification	published	Specifies the system architecture for Urban Guided Transport Management and Command/Control systems (UGTMS) as defined in IEC 62290-1 and IEC 62290-2, and the allocation of functions and requirements defined in IEC 62290-2 to the different UGTMS subsystems (designated as system constituents in IEC 62290-1 and IEC 62290-2), for use in urban guided passenger transport lines and networks.	
42.	ISO/TC 22/SC 32 , Electrical and electronic components and general system aspects	ISO/PAS 5112:2022 Road vehicles — Guidelines for auditing cybersecurity engineering	published	In addition to the guidelines in ISO 19011, this document provides guidelines to organizations that contribute to the achievement of road vehicle cybersecurity throughout the supply chain on: <ul style="list-style-type: none"> — managing an audit programme for a cybersecurity management system (CSMS); — conducting organizational CSMS audits; — competencies of CSMS auditors; and — providing evidence during CSMS audits. Elements of the CSMS are based on the processes described in ISO/SAE 21434. This document is applicable to those needing to understand or conduct internal or external audits of a CSMS or to manage a CSMS audit programme. This document does not provide guidelines on cybersecurity assessments.	
43.	ISO/TC 22/SC 32 , Electrical and electronic components and general system aspects	ISO/SAE 21434:2021 Road vehicles — Cybersecurity engineering	published	Specifies requirements for cybersecurity risk management regarding engineering for concept, 3 development, production, operation, maintenance, and decommissioning for road vehicle electrical and electronic (E/E) 4 systems, including their components and interfaces. A framework is defined that includes requirements for cybersecurity processes and a common language for 6 communicating and managing cybersecurity risk.	
44.	ISO/TC 22 Road vehicles	ISO TR 4804 Road vehicles — Safety and cybersecurity for automated driving systems — Design, verification and validation	published	Describes steps for developing and validating automated driving systems based on basic safety principles derived from worldwide applicable publications. It considers safety- and cybersecurity-by-design, as well as verification and validation methods for automated driving systems focused on vehicles with level 3 and level 4 features according to SAE J3016:2018. In addition, it outlines cybersecurity considerations intersecting with objectives for safety of automated driving systems.	

	Standardization Body	Title	Status	Summary	CitySCAPE Action
45.	ISO/TC 204 , Intelligent Transport Systems	ISO 10711:2012, Intelligent Transport Systems — Interface Protocol and Message Set Definition between Traffic Signal Controllers and Detectors	published	Defines protocols and message sets between traffic detectors and traffic signal controllers.	
46.	ISO/TC 204 , Intelligent Transport Systems	ISO/TR 10992:2011, Intelligent transport systems — Use of nomadic and portable devices to support ITS service and multimedia provision in vehicles	published	Specifies the introduction of multimedia and telematics nomadic devices in the public transport and automotive world to support intelligent transport systems (ITS) service provisions and multimedia use such as passenger information, automotive information, driver advisory and warning systems, and entertainment system interfaces to ITS service providers and motor vehicle communication networks.	
47.	ISO/TC 204 , Intelligent Transport Systems	ISO/TR 10992-2:2017, Intelligent transport systems — Use of nomadic and portable devices to support ITS service and multimedia provision in vehicles — Part 2: Definition and use cases for mobile service convergence	published	Specifies the introduction of multimedia and telematics nomadic devices in the public transport and automotive world to support intelligent transport systems (ITS) service provisions and multimedia use such as passenger information, automotive information, driver advisory and warning systems, and entertainment system interfaces to ITS service providers and motor vehicle communication networks. This document focuses on the convergence software framework to identify mobile cloud connectivity services while driving utilizing nomadic device application for intelligent transport systems (ITS) technologies in vehicles.	
48.	ISO/TC 204 , Intelligent Transport Systems	ISO/TR 12859:2009, Intelligent transport systems — System architecture — Privacy aspects in ITS standards and systems	published	Gives general guidelines to developers of intelligent transport systems (ITS) standards and systems on data privacy aspects and associated legislative requirements for the development and revision of ITS standards and systems.	
49.	ISO/TC 204 , Intelligent Transport Systems	ISO/TR 13184-1:2013, Intelligent transport systems — Guidance protocol via personal ITS station for advisory safety systems — Part 1: General information and use case definitions	published	Specifies guidance information protocol to provide real-time decision support system to drivers or pedestrians using personal ITS stations.	

	Standardization Body	Title	Status	Summary	CitySCAPE Action
50.	ISO/TC 204 , Intelligent Transport Systems	ISO 13184-2:2016, Intelligent transport systems (ITS) — Guidance protocol via personal ITS station for advisory safety systems — Part 2: Road guidance protocol (RGP) requirements and specification	published	Specifies the road guidance use cases on the DXM to provide the real-time decision support system to drivers or pedestrians using P-ITS-S.	
51.	ISO/TC 204 , Intelligent Transport Systems	ISO 13184-3:2017, Intelligent transport systems (ITS) — Guidance protocol via personal ITS station for advisory safety systems — Part 3: Road guidance protocol (RGP) conformance test specification	published	Specifies conformance tests for a self-conformance assessment of the supplier's P-ITS-S system.	
52.	ISO/TC 204 , Intelligent Transport Systems	ISO/TR 13185-1:2012, Intelligent transport systems — Vehicle interface for provisioning and support of ITS services — Part 1: General information and use case definition	published	Specifies the communications architecture and generic protocol to provide and maintain ITS services to travellers (including drivers, passengers and pedestrians), using nomadic and portable devices.	
53.	ISO/TC 204 , Intelligent Transport Systems	ISO 13185-2:2015, Intelligent transport systems — Vehicle interface for provisioning and support of ITS services — Part 2: Unified gateway protocol (UGP) requirements and specification for vehicle ITS station gateway (V-ITS-SG) interface	published	Specifies the requirements of an ASN.1-based protocol between a vehicle-ITS-Station Gateway (V-ITS-SG) and a nomadic and/or mobile device (ND) to easily exchange vehicle information data.	

	Standardization Body	Title	Status	Summary	CitySCAPE Action
54.	ISO/TC 204 , Intelligent Transport Systems	ISO 13185-3:2018, Intelligent transport systems — Vehicle interface for provisioning and support of ITS Services — Part 3: Unified vehicle interface protocol (UVIP) server and client API specification	published	Specifies the server and client APIs of the Unified Gateway Protocol (UGP).	
55.	ISO/TC 204 , Intelligent Transport Systems	ISO 13185-4:2020, Intelligent transport systems — Vehicle interface for provisioning and support of ITS Services — Part 4: Unified vehicle interface protocol (UVIP) conformance test specification	published	Specifies a conformance test for a UVIP server and client system developer assessment of self-conformance of the supplier's UVIP server and client system.	
56.	ISO/TC 204 , Intelligent Transport Systems	ISO 14296:2016, Intelligent transport systems — Extension of map database specifications for applications of cooperative ITS	published	Provides the map-related functional requirements, data model (logical data model/logical data organization), and data elements for those applications of cooperative ITS that require information derived from map databases.	
57.	ISO/TC 204 , Intelligent Transport Systems	ISO 14813-1:2015, Intelligent transport systems — Reference model architecture(s) for the ITS sector — Part 1: ITS service domains, service groups and services	published	Provides a description of the primary services that an ITS implementation can provide to ITS users.	
58.	ISO/TC 204 , Intelligent Transport Systems	ISO 14813-5:2020, Intelligent transport systems — Reference model architecture(s) for the ITS sector — Part 5: Requirements for architecture description in ITS standards	published	Defines documentation rules for standards that define interfaces between or among system elements of an ITS reference architecture.	

	Standardization Body	Title	Status	Summary	CitySCAPE Action
59.	ISO/TC 204 , Intelligent Transport Systems	ISO 14813-6:2017, Intelligent transport systems — Reference model architecture(s) for the ITS sector — Part 6: Use of ASN.1	published	Provides a formal means to achieve consistency in the use of ASN.1 when specifying data types that are to be used in ITS International Standards.	
60.	ISO/TC 204 , Intelligent Transport Systems	ISO 14814:2006, Road transport and traffic telematics — Automatic vehicle and equipment identification — Reference architecture and terminology	published	Establishes a common framework to achieve unambiguous identification in ITS/RTTT: AVI/AEI applications.	
61.	ISO/TC 204 , Intelligent Transport Systems	ISO 14815:2005, Road transport and traffic telematics — Automatic vehicle and equipment identification — System specifications	published	Defines a generic AVI/AEI System specification for nominal AVI/AEI to provide an enabling International Standard, which, whilst allowing the system specifier to determine the performance levels and operating conditions, provides a framework for nominal interoperability.	
62.	ISO/TC 204 , Intelligent Transport Systems	ISO 14816:2005/Amd.1:2019, Road transport and traffic telematics — Automatic vehicle and equipment identification — Numbering and data structure AMENDMENT 1	published	Defines a generic AVI/AEI System specification for nominal AVI/AEI to provide an enabling International Standard, which, whilst allowing the system specifier to determine the performance levels and operating conditions, provides a framework for nominal interoperability.	
63.	ISO/TC 204 , Intelligent Transport Systems	ISO 14817-1:2015, Intelligent transport systems — ITS central data dictionaries — Part 1: Requirements for ITS data definitions	published	Specifies the logical structure (framework) and the data content (substance) of intelligent transport systems (ITS) data dictionaries (DDs).	
64.	ISO/TC 204 , Intelligent Transport Systems	ISO 14817-2:2015, Intelligent transport systems — ITS central data dictionaries — Part 2: Governance of the Central ITS Data Concept Registry	published	Specifies the registration process to enter data concepts into the Central ITS Data Concept Registry (CIDCR).	

	Standardization Body	Title	Status	Summary	CitySCAPE Action
65.	ISO/TC 204 , Intelligent Transport Systems	ISO 14817-3:2017, Intelligent transport systems — ITS data dictionaries — Part 3: Object identifier assignments for ITS data concepts	published	Specifies how to assign an object identifier to a data concept under the “its” arc of the international object identifier tree.	
66.	ISO/TC 204 , Intelligent Transport Systems	ISO 14819-1:2013, Intelligent transport systems — Traffic and travel information messages via traffic message coding — Part 1: Coding protocol for Radio Data System — Traffic Message Channel (RDS-TMC) using ALERT-C	published	The ALERT-C protocol defined in this part of ISO 14819 supports a data broadcasting service for travellers, providing information about many kinds of traffic and travel events. Messages include traffic incident information relating to national and regional routes and some urban roads and other information required by a traveller, such as roadworks and weather information.	
67.	ISO/TC 204 , Intelligent Transport Systems	ISO 14819-2:2013, Intelligent transport systems — Traffic and travel information messages via traffic message coding — Part 2: Event and information codes for Radio Data System — Traffic Message Channel (RDS-TMC) using ALERT-C	published	This part of ISO 14819 defines the ‘Events List’ to be used in coding those messages.	
68.	ISO/TC 204 , Intelligent Transport Systems	ISO 14819-3:2013, Intelligent transport systems — Traffic and travel information messages via traffic message coding — Part 3: Location referencing for Radio Data System — Traffic Message Channel (RDS-TMC) using ALERT-C	published	Sets out ways of specifying places and positions in traffic and travel information messages, including RDS-TMC messages (the Radio Data System - Traffic Message Channel).	

	Standardization Body	Title	Status	Summary	CitySCAPE Action
69.	ISO/TC 204 , Intelligent Transport Systems	ISO 14819-6:2006, Traffic and Traveller Information (TTI) — TTI messages via traffic message coding — Part 6: Encryption and conditional access for the Radio Data System — Traffic Message Channel ALERT C coding	published	Sstablishes a method of encrypting certain elements of the ALERT-C coded data carried in the RDS-TMC type 8A data group, such that without application by a terminal or receiver of an appropriate key, the information conveyed is virtually worthless.	
70.	ISO/TC 204 , Intelligent Transport Systems	ISO 15075:2003, Transport information and control systems — In-vehicle navigation systems — Communications message set requirements	published	Specifies message content and format utilized by in-vehicle navigation systems. Its emphasis is on messages that are required to generate or enhance routing instructions.	
71.	ISO/TC 204 , Intelligent Transport Systems	ISO 15622:2018, Intelligent transport systems — Adaptive cruise control systems — Performance requirements and test procedures	published	Contains the basic control strategy, minimum functionality requirements, basic driver interface elements, minimum requirements for diagnostics and reaction to failure, and performance test procedures for Adaptive Cruise Control (ACC) systems.	
72.	ISO/TC 204 , Intelligent Transport Systems	ISO 15623:2013, Intelligent transport systems — Forward vehicle collision warning systems — Performance requirements and test procedures	published	Specifies performance requirements and test procedures for systems capable of warning the driver of a potential rear-end collision with other vehicles ahead of the subject vehicle while it is operating at ordinary speed.	
73.	ISO/TC 204 , Intelligent Transport Systems	ISO/TS 15624:2001, Transport information and control systems — Traffic Impediment Warning Systems (TIWS) — System requirements	published	Specifies system requirements for Traffic Impediment Warning Systems (TIWS).	
74.	ISO/TC 204 , Intelligent Transport Systems	ISO 15628:2013, Intelligent transport systems — Dedicated short range communication (DSRC) — DSRC application layer	published	Specifies the application layer core which provides communication tools for applications based on DSRC.	

	Standardization Body	Title	Status	Summary	CitySCAPE Action
75.	ISO/TC 204 , Intelligent Transport Systems	ISO 17185-1:2014, Intelligent transport systems — Public transport user information — Part 1: Standards framework for public information systems	published	Defines the framework for the realization of efficient public transport user information provision to surface public transport users including international worldwide travellers.	
76.	ISO/TC 204 , Intelligent Transport Systems	ISO/TR 17185-2:2015, Intelligent transport systems — Public transport user information — Part 2: Public transport data and interface standards catalogue and cross references	published	Compares and contrasts public transport standards that were developed by different regions and countries.	
77.	ISO/TC 204 , Intelligent Transport Systems	ISO/TR 17185-3:2015, Intelligent transport systems — Public transport user information — Part 3: Use cases for journey planning systems and their interoperation	published	Defines basic requirements for implementing the journey planning system, from the viewpoint that the public transport users should be provided with convenient tool to make his or her journey more efficient ones.	
78.	ISO/TC 204 , Intelligent Transport Systems	ISO 17267:2009, Intelligent transport systems — Navigation systems — Application programming interface (API)	published	Specifies an application programming interface (API) for navigation systems.	
79.	ISO/TC 204 , Intelligent Transport Systems	ISO 17361:2017, Intelligent transport systems — Lane departure warning systems — Performance requirements and test procedures	published	Specifies the definition of the system, classification, functions, human-machine interface (HMI) and test methods for lane departure warning systems.	
80.	ISO/TC 204 , Intelligent Transport Systems	ISO/TR 17384:2008, Intelligent transport systems — Interactive centrally determined route guidance (CDRG) — Air interface message set, contents and format	published	Describes the message contents and format of the air interface between the infrastructure and the in-vehicle unit in the Interactive CDRG system.	

	Standardization Body	Title	Status	Summary	CitySCAPE Action
81.	ISO/TC 204 , Intelligent Transport Systems	ISO 17386:2010, Transport information and control systems — Manoeuvring Aids for Low Speed Operation (MALSO) — Performance requirements and test procedures	published	Specifies minimum functionality requirements which the driver can generally expect of the device, i.e. detection of and information on the presence of relevant obstacles within a defined (short) detection range.	
82.	ISO/TC 204 , Intelligent Transport Systems	ISO 17387:2008, Intelligent transport systems — Lane change decision aid systems (LCDAS) — Performance requirements and test procedures	published	Specifies system requirements and test methods for Lane Change Decision Aid Systems (LCDAS).	
83.	ISO/TC 204 , Intelligent Transport Systems	ISO 17438-1:2016, Intelligent transport systems — Indoor navigation for personal and vehicle ITS station — Part 1: General information and use case definition	published	Specifies the indoor navigation system architecture including additional components that are added to the existing ITS system and use cases in providing indoor navigation to various types of users including drivers, passengers, and pedestrians using personal and vehicle ITS stations.	
84.	ISO/TC 204 , Intelligent Transport Systems	ISO 17438-4:2019, Intelligent transport systems — Indoor navigation for personal and vehicle ITS station — Part 4: Requirements and specifications for interface between personal/vehicle and central ITS stations	published	Defines detailed use cases, requirements and message specifications for supporting indoor navigation functionality between a personal/vehicle (P/V) ITS station and a central ITS station.	
85.	ISO/TC 204 , Intelligent Transport Systems	ISO/TR 18317:2017, Intelligent transport systems — Pre-emption of ITS communication networks for disaster and emergency communication — Use case scenarios	published	Provides the outcome of discussions on use case scenarios and assumed requirements for using ad-hoc wireless networks under disaster and emergency conditions including related priority, security and urgency aspects of communication requirements.	
86.	ISO/TC 204 , Intelligent Transport Systems	ISO 18682:2016, Intelligent transport systems — External hazard detection and notification systems — Basic requirements	published	Specifies basic requirements for systems to execute notifications such as warning and awareness messages to provide hazard information to a driver.	

	Standardization Body	Title	Status	Summary	CitySCAPE Action
87.	ISO/TC 204 , Intelligent Transport Systems	ISO/TR 19083-1:2016, Intelligent transport systems — Emergency evacuation and disaster response and recovery — Part 1: Framework and concept of operation	published	Defines the framework and concept of operation for the use of public transport during an emergency evacuation or large scale disaster.	
88.	ISO/TC 204 , Intelligent Transport Systems	ISO 19237:2017, Intelligent transport systems — Pedestrian detection and collision mitigation systems (PDCMS) — Performance requirements and test procedures	published	Specifies the concept of operation, minimum functionality, system requirements, system interfaces, and test procedures for Pedestrian Detection and Collision Mitigation Systems (PDCMS).	
89.	ISO/TC 204 , Intelligent Transport Systems	ISO/TS 19468:2019, Intelligent transport systems — Data interfaces between centres for transport information and control systems — Platform independent model specifications for data exchange protocols for transport information and control systems	published	Defines and specifies component facets supporting the exchange and shared use of data and information in the field of traffic and travel.	
90.	ISO/TC 204 , Intelligent Transport Systems	ISO/TR 20529-1:2017, Intelligent transport systems — Framework for green ITS (G-ITS) standards — Part 1: General information and use case definitions	published	Provides the framework guideline for identifying cost-effective technologies and related standards required to deploy, manage and operate sustainable “green” intelligent transport systems (ITS) technologies in surface transportations with eco-mobility.	
91.	ISO/TC 204 , Intelligent Transport Systems	ISO 20529-2:2021, Intelligent transport systems — Framework for Green ITS (G-ITS) standards — Part 2: Integrated mobile service applications	published	Provides the framework guideline for identifying cost-effective technologies and related standards required to deploy, manage and operate sustainable “green” intelligent transport systems (ITS) technologies in surface transportations with eco-mobility, which would undertake joint work with ISO Technical Committee 204 (ISO/TC204) – Intelligent Transport Systems (ITS) to identify. These ITS technologies can increase operational efficiencies and unlock enhanced transportation safety and eco-mobility applications.	

	Standardization Body	Title	Status	Summary	CitySCAPE Action
92.	ISO/TC 204 , Intelligent Transport Systems	ISO 20900:2019, Intelligent transport systems — Partially automated parking systems (PAPS) — Performance requirements and test procedures	published	Establishes minimum functionality requirements that the driver can expect and the manufacturer needs to take into account.	
93.	ISO/TC 204 , Intelligent Transport Systems	ISO 20901:2020, Intelligent transport systems — Emergency electronic brake light systems (EEBL) — Performance requirements and test procedures	published	Contains the basic alert strategy, minimum functionality requirements, basic driver interface elements, minimum requirements for diagnostics and reaction to failure, and performance test procedures for Emergency Electronic Brake Light systems (EEBL).	
94.	ISO/TC 204 , Intelligent Transport Systems	ISO/TS 21177:2019, Intelligent transport systems — ITS station security services for secure session establishment and authentication between trusted devices	published	Contains specifications for a set of ITS station security services required to ensure the authenticity of the source and integrity of information exchanged between trusted entities.	
95.	ISO/TC 204 , Intelligent Transport Systems	ISO/TS 21185:2019, Intelligent transport systems — Communication profiles for secure connections between trusted devices	published	Specifies a methodology to define ITS-S communication profiles (ITS-SCPs) based on standardized communication protocols to interconnect trusted devices.	
96.	ISO/TC 204 , Intelligent Transport Systems	ISO 22839:2013, Intelligent transport systems — Forward vehicle collision mitigation systems — Operation, performance, and verification requirements	published	Specifies the concept of operation, minimum functionality, system requirements, system interfaces, and test methods for Forward Vehicle Collision Mitigation Systems (FVCMS). It specifies the behaviors that are required for FVCMS, and the system test criteria necessary to verify that a given implementation meets the requirements of ISO 22839:2013.	
97.	ISO/TC 204 , Intelligent Transport Systems	ISO 24014-1:2015, (ISO/DIS 24014-1:2020) Public transport — Interoperable fare management system — Part 1: Architecture	published	Objective of the ISO 24014 series of standards: provide the basis for the development of multi-operator/multi-service Interoperable public surface (including subways) transport Fare Management Systems (IFMSs) on a national and international level.	

	Standardization Body	Title	Status	Summary	CitySCAPE Action
98.	ISO/TC 204 , Intelligent Transport Systems	ISO/TR 24014-2:2013, Public transport — Interoperable fare management system — Part 2: Business practices	published	See above	
99.	ISO/TC 204 , Intelligent Transport Systems	ISO/TR 24014-3:2013, Public transport — Interoperable fare management system — Part 3: Complementary concepts to Part 1 for multi-application media	published	See above	
100.	ISO/TC 204 , Intelligent Transport Systems	ISO 24100:2010, Intelligent transport systems — Basic principles for personal data protection in probe vehicle information services	published	States the basic rules to be observed by service providers who handle personal data in probe vehicle information services.	
101.	ISO/TC 204 , Intelligent Transport Systems	ISO 24102-1:2018, Intelligent transport systems — ITS station management — Part 1: Local management	published	Provides specifications for intelligent transport systems (ITS) station management to be in conformance with the ITS station reference architecture.	
102.	ISO/TC 204 , Intelligent Transport Systems	ISO 24102-2:2018, Intelligent transport systems — ITS station management — Part 2: Remote management of ITS-SCUs	published	Provides specifications for intelligent transport systems (ITS) station management to conform with the ITS station reference architecture.	
103.	ISO/TC 204 , Intelligent Transport Systems	ISO 24102-3:2018, Intelligent transport systems — ITS station management — Part 3: Service access points	published	Specifies the management service access points.	
104.	ISO/TC 204 , Intelligent Transport Systems	ISO 24102-4:2018, Intelligent transport systems — ITS station management — Part 4: Station-internal management communications	published	Provides specifications for secure ITS station-internal management communications.	

	Standardization Body	Title	Status	Summary	CitySCAPE Action
105.	ISO/TC 204 , Intelligent Transport Systems	ISO 24534-1:2010, Automatic vehicle and equipment identification — Electronic registration identification (ERI) for vehicles — Part 1: Architecture	published	Provides requirements for electronic registration identification (ERI) that are based on an identifier assigned to a vehicle (e.g. for recognition by national authorities)	
106.	ISO/TC 204 , Intelligent Transport Systems	ISO 24534-2:2010, Automatic vehicle and equipment identification — Electronic registration identification (ERI) for vehicles — Part 2: Operational requirements	published	Defines the operational requirements for the remaining parts of ISO 24534 and the more limited but relevant provisions of ISO 24535.	
107.	ISO/TC 204 , Intelligent Transport Systems	ISO 24534-3:2016, Intelligent transport systems — Automatic vehicle and equipment identification — Electronic registration identification (ERI) for vehicles — Part 3: Vehicle data	published	Defines the vehicle identification data.	
108.	ISO/TC 204 , Intelligent Transport Systems	ISO 24534-4:2010, Automatic vehicle and equipment identification — Electronic registration identification (ERI) for vehicles — Part 4: Secure communications using asymmetrical techniques	published	Specifies the interfaces for a secure exchange of data between an ERT and an ERI reader or ERI writer in or outside the vehicle using asymmetric encryption techniques.	
109.	ISO/TC 204 , Intelligent Transport Systems	ISO 24534-5:2011, Intelligent transport systems — Automatic vehicle and equipment identification — Electronic Registration Identification (ERI) for vehicles — Part 5: Secure communications using symmetrical techniques	published	Specifies the interfaces for a secure exchange of data between the electronic registration tag (ERT), which is the onboard device containing the ERI data, and the ERI reader or ERI writer in or outside the vehicle using symmetric encryption techniques.	

	Standardization Body	Title	Status	Summary	CitySCAPE Action
110.	ISO/TC 204 , Intelligent Transport Systems	ISO 24535:2007, Intelligent transport systems — Automatic vehicle identification — Basic electronic registration identification (Basic ERI)	published	Defines the specification of a unique vehicle identifier (using an International Standard, or non-standard, data concept), “basic ERI” functional capabilities, selectable for different “basic ERI” applications, and minimum data interoperability requirements between basic electronic registration tags (ERTs) and electronic registration readers (ERRs).	
111.	ISO/TC 204 , Intelligent Transport Systems	ISO 24978:2009, Intelligent transport systems — ITS Safety and emergency messages using any available wireless media — Data registry procedures	published	Provides a standardized set of protocols, parameters, and a method of management of an updateable "Data Registry" to provide application layers for "ITS Safety messages" using any available wireless media.	
112.	ISO/TC 204 , Intelligent Transport Systems	ISO 26684:2015, Intelligent transport systems (ITS) — Cooperative intersection signal information and violation warning systems (CIWS) — Performance requirements and test procedures	published	Specifies the concept of operation, system requirements, and test methods for cooperative intersection signal information and violation warning systems (CIWS) at signalized intersections.	
113.	ISO TC 241 , Road traffic safety management systems	ISO 39001:2012, Road traffic safety (RTS) management systems - Requirements with guidance for use	published	Specifies requirements for a road traffic safety (RTS) management system to enable an organization that interacts with the road traffic system to reduce death and serious injuries related to road traffic crashes which it can influence.	
114.	ISO TC 241 , Road traffic safety management systems	ISO 39002:2020, Road traffic safety — Good practices for implementing commuting safety management	published	Provides guidelines for good practices that can be adopted by organizations for the implementation of commuting safety management.	
115.	ISO/TC 268 , Sustainable cities and communities	ISO 37120 Sustainable cities and communities — Indicators for city services and quality of life	published	Defines and establishes methodologies for a set of indicators to steer and measure the performance of city services and quality of life.	
116.	ISO/TC 268 , Sustainable cities and communities	ISO 37122 Sustainable cities and communities — Indicators for smart cities	published	Specifies and establishes definitions and methodologies for a set of indicators for smart cities.	

	Standardization Body	Title	Status	Summary	CitySCAPE Action
117.	ISO/TC 268 , Sustainable cities and communities	ISO 37123 Sustainable cities and communities — Indicators for resilient cities	published	Defines and establishes definitions and methodologies for a set of indicators on resilience in cities.	
118.	ISO/TC 268/SC 1 , Smart community infrastructures	ISO 37154 Smart community infrastructures — Best practice guidelines for transportation	published	Provides general guidance on the planning, design, development, organization, monitoring, maintenance and improvement process of smart transportation systems and infrastructures, which can help promote solutions for intra- and inter-city issues, i.e. for issues both within and outside the city that impact quality of life, the environment or any other areas of city performance.	
119.	ISO/TC 268/SC 1 , Smart community infrastructures	ISO 37157 Smart community infrastructures — Smart transportation for compact cities	published	Describes criteria to help plan or organize smart transportation for compact cities.	
120.	ISO/TC 268/SC 1 , Smart community infrastructures	ISO 37158 Smart community infrastructures — Smart transportation using battery-powered buses for passenger services	published	Specifies a procedure for the introduction of smart transportation to city centres by means of battery-powered buses.	
121.	ISO/TC 268/SC 1 , Smart community infrastructures	ISO 37159 Smart community infrastructures — Smart transportation for rapid transit in and between large city zones and their surrounding areas	published	Specifies a procedure to organize smart transportation that enables one-day trips by citizens between cities and in a large city zone, including its surrounding areas, and conveys a large number of people at a high frequency in a short time over distances of up to 1 000 km.	
122.	ISO/TC 268/SC 1 , Smart community infrastructures	ISO 37161 Smart community infrastructures — Guidance on smart transportation for energy saving in transportation services	published	Provides guidance on reducing the energy consumed by transportation for passengers, delivery items, freight and postal item services in cities and city zones.	
123.	ISO/TC 268/SC 1 , Smart community infrastructures	ISO 37162 Smart community infrastructures — Smart transportation for newly developing areas	published	Specifies a procedure to arrange smart transportation for newly developing areas, including transportation services between the area and existing city centres.	

	Standardization Body	Title	Status	Summary	CitySCAPE Action
124.	ISO/TC 268/SC 1 , Smart community infrastructures	ISO 37163 Smart community infrastructures — Smart transportation for parking lot allocation in cities	published	Specifies procedures for installing and organizing smart transportation for parking lot allocation for drivers in cities.	
125.	ISO/TC 268/SC 1 , Smart community infrastructures	ISO 37165 Smart community infrastructures — Guidance on smart transportation with the use of digitally processed payment (d-payment)	published	Provides guidance on how to organize and implement smart transportation by digitally processed payment (d-payment) in order to provide a safe, convenient payment method for citizens and city visitors in transportation and its related or additional services.	
126.	ISO/TC 268/SC 1 , Smart community infrastructures	ISO/DIS 37180, Smart community infrastructures — Guidance on smart transportation with QR code identification and authentication in transportation and its related or additional services	published	Provides guidance on transportation and its related or additional services using quick response (QR) codes for identification and authentication in data transfer, in order to make their services both convenient and advantageous for customers and service agents while protecting them from cheating and illegal action in data transfer.	

	Standardization Body	Title	Status	Summary	CitySCAPE Action
127.	ISO/IEC JTC 1 , Information Technology	ISO/IEC 20922, Information technology -- Message Queuing Telemetry Transport (MQTT) v3.1.1	published	<p>ISO/IEC 20922:2016 is a Client Server publish/subscribe messaging transport protocol. It is light weight, open, simple, and designed so as to be easy to implement. These characteristics make it ideal for use in many situations, including constrained environments such as for communication in Machine to Machine (M2M) and Internet of Things (IoT) contexts where a small code footprint is required and/or network bandwidth is at a premium. The protocol runs over TCP/IP, or over other network protocols that provide ordered, lossless, bi-directional connections. Its features include:</p> <ul style="list-style-type: none"> - Use of the publish/subscribe message pattern which provides one-to-many message distribution and decoupling of applications. - A messaging transport that is agnostic to the content of the payload. - Three qualities of service for message delivery: <ul style="list-style-type: none"> "At most once", where messages are delivered according to the best efforts of the operating environment. Message loss can occur. This level could be used, for example, with ambient sensor data where it does not matter if an individual reading is lost as the next one will be published soon after. "At least once", where messages are assured to arrive but duplicates can occur. "Exactly once", where message are assured to arrive exactly once. This level could be used, for example, with billing systems where duplicate or lost messages could lead to incorrect charges being applied. 	

	Standardization Body	Title	Status	Summary	CitySCAPE Action
128.	ISO/IEC JTC 1/SC 17 , Cards and security devices for personal identification	ISO/IEC 7816, Identification cards — Integrated circuit cards	published	<p>Series of standards, related to electronic identification cards with contacts, especially smart cards, and contactless mobile devices:</p> <p>ISO/IEC 7816-1:2011 Part 1: Cards with contacts—Physical characteristics</p> <p>ISO/IEC 7816-2:2007 Part 2: Cards with contacts—Dimensions and location of the contacts</p> <p>ISO/IEC 7816-3:2006 Part 3: Cards with contacts—Electrical interface and transmission protocols</p> <p>ISO/IEC 7816-4:2013 Part 4: Organization, security and commands for interchange</p> <p>ISO/IEC 7816-5:2004 Part 5: Registration of application providers</p> <p>ISO/IEC 7816-6:2016 Part 6: Interindustry data elements for interchange</p> <p>ISO/IEC 7816-7:1999 Part 7: Interindustry commands for Structured Card Query Language (SCQL)</p> <p>ISO/IEC 7816-8:2016 Part 8: Commands and mechanisms for security operations</p> <p>ISO/IEC 7816-9:2017 Part 9: Commands for card management</p> <p>ISO/IEC 7816-10:1999 Part 10: Electronic signals and answer to reset for synchronous cards</p> <p>ISO/IEC 7816-11:2017 Part 11: Personal verification through biometric methods</p> <p>ISO/IEC 7816-12:2005 Part 12: Cards with contacts—USB electrical interface and operating procedures</p> <p>ISO/IEC 7816-13:2007 Part 13: Commands for application management in a multi-application environment</p> <p>ISO/IEC 7816-15:2016 Part 15: Cryptographic information application</p>	

	Standardization Body	Title	Status	Summary	CitySCAPE Action
129.	ISO/IEC JTC 1, Information technology/SC 17 , Cards and security devices for personal identification	ISO/IEC 10373, Cards and security devices for personal identification — Test methods	published	Series of standards, describing test methods of cards and security devices for personal identification: ISO/IEC 10373-1:2020 Cards and security devices for personal identification — Test methods — Part 1: General characteristics ISO/IEC 10373-2:2015 Identification cards — Test methods — Part 2: Cards with magnetic stripes ISO/IEC 10373-3:2018 Identification cards — Test methods — Part 3: Integrated circuit cards with contacts and related interface devices ISO/IEC 10373-5:2014 Identification cards — Test methods — Part 5: Optical memory cards ISO/IEC 10373-6:2020 Cards and security devices for personal identification — Test methods — Part 6: Contactless proximity objects ISO/IEC 10373-6:2020/AMD 2:2020 Cards and security devices for personal identification — Test methods — Part 6: Contactless proximity objects — Amendment 2: Enhancements for harmonization ISO/IEC 10373-7:2019 Cards and security devices for personal identification — Test methods — Part 7: Contactless vicinity objects ISO/IEC 10373-8:2011 Identification cards — Test methods — Part 8: USB-ICC ISO/IEC 10373-9:2011 Identification cards — Test methods — Part 9: Optical memory cards — Holographic recording method	
130.	ISO/IEC JTC 1/SC 17 , Cards and security devices for personal identification	ISO/IEC 11693, Identification cards — Optical memory cards	published	Series of standards, describing aspects of Optical Memory Cards: ISO/IEC 11693-1:2012 Identification cards — Optical memory cards — Part 1: General characteristics ISO/IEC 11693-2:2009 Identification cards — Optical memory cards — Part 2: Co-existence of optical memory with other machine-readable technologies ISO/IEC 11693-3:2015 Identification cards — Optical memory cards — Part 3: Authentication techniques	
131.	ISO/IEC JTC 1/SC 17 , Cards and security devices for personal identification	ISO/IEC 15457, Identification cards — Thin flexible cards	published	Series of standards, describing various aspects of Thin Flexible Cards: ISO/IEC 15457-3:2008 Identification cards — Thin flexible cards — Part 3: Test methods ISO/IEC 15457-2:2007 Identification cards — Thin flexible cards — Part 2: Magnetic recording technique ISO/IEC 15457-1:2008 Identification cards — Thin flexible cards — Part 1: Physical characteristics	

	Standardization Body	Title	Status	Summary	CitySCAPE Action
132.	ISO/IEC JTC 1/SC 17 , Cards and security devices for personal identification	ISO/IEC 15693, Cards and security devices for personal identification - Contactless vicinity objects	published	Series of standards covering various aspects of Contactless vicinity objects: ISO/IEC 15693-1:2018 Cards and security devices for personal identification — Contactless vicinity objects — Part 1: Physical characteristics ISO/IEC 15693-2:2019 Cards and security devices for personal identification — Contactless vicinity objects — Part 2: Air interface and initialization ISO/IEC 15693-3:2019 Cards and security devices for personal identification — Contactless vicinity objects — Part 3: Anticollision and transmission protocol	
133.	ISO/IEC JTC 1/SC 17 , Cards and security devices for personal identification	ISO/IEC 18013, Personal identification — ISO-compliant driving licence	published	Series of standards covering various aspects of ISO-compliant driving licence: ISO/IEC 18013-1:2018 Information technology — Personal identification — ISO-compliant driving licence — Part 1: Physical characteristics and basic data set ISO/IEC 18013-2:2020 Personal identification — ISO-compliant driving licence — Part 2: Machine-readable technologies ISO/IEC 18013-3:2017 Information technology — Personal identification — ISO-compliant driving licence — Part 3: Access control, authentication and integrity validation ISO/IEC 18013-4:2019 Personal identification — ISO-compliant driving licence — Part 4: Test methods	

	Standardization Body	Title	Status	Summary	CitySCAPE Action
134.	ISO/IEC JTC 1/SC 17 , Cards and security devices for personal identification	ISO/IEC 14443, Cards and security devices for personal identification — Contactless proximity objects	published	Series of standards covering various aspects of Contactless proximity objects: ISO/IEC 14443-1:2018 Cards and security devices for personal identification — Contactless proximity objects — Part 1: Physical characteristics ISO/IEC 14443-2:2020 Cards and security devices for personal identification — Contactless proximity objects — Part 2: Radio frequency power and signal interface ISO/IEC 14443-3:2018 Cards and security devices for personal identification — Contactless proximity objects — Part 3: Initialization and anticollision ISO/IEC 14443-3:2018/AMD 2:2020 Cards and security devices for personal identification — Contactless proximity objects — Part 3: Initialization and anticollision — Amendment 2: Enhancements for harmonization ISO/IEC 14443-4:2018 Cards and security devices for personal identification — Contactless proximity objects — Part 4: Transmission protocol ISO/IEC 14443-4:2018/AMD 2:2020 Cards and security devices for personal identification — Contactless proximity objects — Part 4: Transmission protocol — Amendment 2: Enhancements for harmonization	
135.	ISO/IEC JTC 1/SC 17 , Cards and security devices for personal identification	ISO/IEC 17839, Information technology — Biometric System-on-Card	published	Series of standards covering various aspects of Biometric System-on-Card: ISO/IEC 17839-1:2014 Information technology — Biometric System-on-Card — Part 1: Core requirements ISO/IEC 17839-2:2015 Information technology — Biometric System-on-Card — Part 2: Physical characteristics ISO/IEC 17839-3:2016 Information technology — Identification cards — Biometric System-on-Card — Part 3: Logical information interchange mechanism	
136.	ISO/IEC JTC 1/SC 27 , Information security, cybersecurity and privacy protection	ISO/IEC 9798 Information technology — Security techniques — Entity authentication (series of standards)	published	This series of standards specifies an authentication model, requirements and constraints for entity authentication mechanisms which use security techniques, the details of the mechanisms and the contents of the authentication exchanges.	

	Standardization Body	Title	Status	Summary	CitySCAPE Action
137.	ISO/IEC JTC 1/SC 27 , Information security, cybersecurity and privacy protection	ISO/IEC 10118-1:2016 Information technology — Security techniques — Hash-functions — Part 1: General	published	ISO/IEC 10118-1:2016 specifies hash-functions and is therefore applicable to the provision of authentication, integrity and non-repudiation services. Hash-functions map strings of bits of variable (but usually upper bounded) length to fixed-length strings of bits, using a specified algorithm.	
138.	ISO/IEC JTC 1/SC 27 , Information security, cybersecurity and privacy protection	ISO/IEC 10118-4:1998 Information technology — Security techniques — Hash-functions — Part 4: Hash-functions using modular arithmetic	published	The hash-functions specified in this part of ISO/IEC 10118, known as MASH-1 and MASH-2 (Modular Arithmetic Secure Hash) are particularly suitable for environments in which implementations of modular arithmetic of sufficient length are already available. The two hash-functions differ only in the exponent used in the round-function.	
139.	ISO/IEC JTC 1/SC 27 , Information security, cybersecurity and privacy protection	ISO/IEC 27001:2013 , Information technology — Security techniques — Information security management systems — Requirements	published	ISO/IEC 27001:2013 specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organization. It also includes requirements for the assessment and treatment of information security risks tailored to the needs of the organization. The requirements set out in ISO/IEC 27001:2013 are generic and are intended to be applicable to all organizations, regardless of type, size or nature.	<p>KSP: The MobSec mobile App defined in Task 3.3 and implemented by SIGLA to build a ‘secure by design’ mobile app for passengers of multimodal local transport is integrated with Kaspersky Mobile Security SDK (KMS-SDK). The Collaborative Threat Intelligence Platform (CTIP) defined in Task 3.3 and implemented by AIRBUS is fed by the Kaspersky Threat Data Feeds. KMS-SDK and Kaspersky Threat Data Feeds are based on services provided by the Kaspersky Security Network (KSN). KSN is ISO-27001 certified in the delivery of malicious and suspicious files.</p> <p>ENG follows ISO 27001:2013 standard through the adoption of the best practices on information security and in particular on information security management</p>

	Standardization Body	Title	Status	Summary	CitySCAPE Action
					<p>systems, from the definition of requirements to the development of all solutions.</p> <p>CSG: Application of this standard to multimodal CPaaS transport system is taken into account as part of T8.2.</p> <p>ED uses ISO 27001:2013 standard as a guide for the specification of the: Design and Implementation of RITA, which is considered a well-documented Information Security Management System (ISMS). Although RITA follows an asset-based risk assessment the tool follows a process-based approach, in line with the model proposed by the ISO standard.</p>
140.	ISO/IEC JTC 1/SC 27 , Information security, cybersecurity and privacy protection	ISO/IEC 27002:2022 , Information technology — Security techniques — Code of practice for information security controls	published	<p>This document provides a reference set of generic information security controls including implementation guidance. This document is designed to be used by organizations:</p> <ul style="list-style-type: none"> a) within the context of an information security management system (ISMS) based on ISO/IEC27001; b) for implementing information security controls based on internationally recognized best practices; c) for developing organization-specific information security management guidelines. 	<p>ACS leverage this code of practice in the design of all its solution to ensure a high level of security is attained.</p> <p>ENG follows ISO 27001:2013 standard through the adoption of the best practices on information security and in particular on information security management systems, from the definition of requirements to the development of all solutions.</p> <p>CSG: Application of this standard to multimodal</p>

	Standardization Body	Title	Status	Summary	CitySCAPE Action
					<p>CPaaS transport system is taken into account as part of T8.2.</p> <p>Additionally to CIS Controls ED leverages the basic concepts introduced by the standard i.e. policy, safeguard or control or countermeasure, risk and information security incident, and through RITA assists organizations to build appropriate countermeasures that when applied help protect their information systems. These controls follow the categorization established in the ISO standard.</p>
141.	ISO/IEC JTC 1/SC 27 , Information security, cybersecurity and privacy protection	ISO/IEC 27003:2017 , Information technology — Security techniques — Information security management systems — Guidance	published	Provides guidance on the requirements for an information security management system (ISMS) as specified in ISO/IEC 27001 and provides recommendations, possibilities and permissions in relation to them.	<p>ACS leverage this guidance in the design of all its solution to ensure a high level of security is attained.</p> <p>ENG follows ISO 27001:2013 standard through the adoption of the best practices on information security and in particular on information security management systems, from the definition of requirements to the development of all solutions.</p> <p>ED uses ISO 27003:2017 standard ISMS requirements, towards the implementation of RITA, which can be used by organisations towards establishing, implementing, monitoring, reviewing,</p>

	Standardization Body	Title	Status	Summary	CitySCAPE Action
					maintaining, and improving their information security in order to achieve their business objectives. RITA is based on a risk assessment and is designed to effectively identify, treat and manage risks. RITA supports the implementation and operation of security measures, appropriate to deal with risks that fall within the specific organizational framework. RITA supports different roles and supports both the information security risk assessment and information security risk treatment by identifying and implementing controls.
142.	ISO/IEC JTC 1/SC 27 , Information security, cybersecurity and privacy protection	ISO/IEC 27004:2016 , Information technology — Security techniques — Information security management — Monitoring, measurement, analysis and evaluation	published	ISO/IEC 27004:2016 provides guidelines intended to assist organizations in evaluating the information security performance and the effectiveness of an information security management system in order to fulfil the requirements of ISO/IEC 27001:2013, 9.1. It establishes: a) the monitoring and measurement of information security performance; b) the monitoring and measurement of the effectiveness of an information security management system (ISMS) including its processes and controls; c) the analysis and evaluation of the results of monitoring and measurement. ISO/IEC 27004:2016 is applicable to all types and sizes of organizations.	

	Standardization Body	Title	Status	Summary	CitySCAPE Action
143.	ISO/IEC JTC 1/SC 27 , Information security, cybersecurity and privacy protection	ISO/IEC 27005:2018 , Information technology — Security techniques — Information security risk management	published	<p>This document provides guidelines for information security risk management.</p> <p>This document supports the general concepts specified in ISO/IEC 27001 and is designed to assist the satisfactory implementation of information security based on a risk management approach.</p> <p>Knowledge of the concepts, models, processes and terminologies described in ISO/IEC 27001 and ISO/IEC 27002 is important for a complete understanding of this document.</p> <p>This document is applicable to all types of organizations (e.g. commercial enterprises, government agencies, non-profit organizations) which intend to manage risks that can compromise the organization's information security.</p> <p>.</p>	ED uses ISO 27005:2018 methodology to help organisations manage their risk. It uses the established definition of risk, i.e. function of probability and impact as well as the related concepts including assets, threats and vulnerabilities. RITA as a risk management tool supports both risk assessment (risk identification, analysis and evaluation) and risk treatment phases of risk management. To support with the preparation of a security plan, RITA allows the definition and selection of countermeasures, controls, safeguards.
144.	ISO/IEC JTC 1/SC 27 , Information security, cybersecurity and privacy protection	ISO/IEC 27006:2015, Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems	published	Specifies requirements and provides guidance for bodies providing audit and certification of an information security management system (ISMS), in addition to the requirements contained within ISO/IEC 17021-1 and ISO/IEC 27001.	
145.	ISO/IEC JTC 1/SC 27 , Information security, cybersecurity and privacy protection	ISO/IEC 27007:2020, Information security, cybersecurity and privacy protection — Guidelines for information security management systems auditing	published	Provides guidance on managing an information security management system (ISMS) audit programme, on conducting audits, and on the competence of ISMS auditors, in addition to the guidance contained in ISO 19011.	

	Standardization Body	Title	Status	Summary	CitySCAPE Action
146.	ISO/IEC JTC 1/SC 27 , Information security, cybersecurity and privacy protection	ISO/IEC TS 27008:2019 , Information technology — Security techniques — Guidelines for the assessment of information security controls	published	Provides guidance on reviewing and assessing the implementation and operation of information security controls, being managed through an Information Security Management System specified by ISO/IEC 27001.	ED uses ISO 27008:2019 as a complementary text to the information security risk management process described in ISO 27005:2018 in the design of RITA, in order to enable organisations using RITA to select countermeasures that are fit for purpose, effective and efficient. Essentially, the process of evaluating technical countermeasures according to ISO 27008:2019 is part of ISO 27002:2013, discussed above.
147.	ISO/IEC JTC 1/SC 27 , Information security, cybersecurity and privacy protection	ISO/IEC 27009:2020 , Information security, cybersecurity and privacy protection — Sector-specific application of ISO/IEC 27001 — Requirements	published	Specifies the requirements for creating sector-specific standards that extend ISO/IEC 27001, and complement or amend ISO/IEC 27002 to support a specific sector (domain, application area or market).	CSG: Application of this standard to multimodal CPaaS transport system is taken into account as part of T8.2 to create a 27001 extension dedicated to urban transport systems

	Standardization Body	Title	Status	Summary	CitySCAPE Action
148.	ISO/IEC JTC 1/SC 27 , Information security, cybersecurity and privacy protection	ISO/IEC 27031:2011 Information technology — Security techniques — Guidelines for information and communication technology readiness for business continuity	published	ISO/IEC 27031:2011 describes the concepts and principles of information and communication technology (ICT) readiness for business continuity, and provides a framework of methods and processes to identify and specify all aspects (such as performance criteria, design, and implementation) for improving an organization's ICT readiness to ensure business continuity. It applies to any organization (private, governmental, and non-governmental, irrespective of size) developing its ICT readiness for business continuity program (IRBC), and requiring its ICT services/infrastructures to be ready to support business operations in the event of emerging events and incidents, and related disruptions, that could affect continuity (including security) of critical business functions. It also enables an organization to measure performance parameters that correlate to its IRBC in a consistent and recognized manner. The scope of ISO/IEC 27031:2011 encompasses all events and incidents (including security related) that could have an impact on ICT infrastructure and systems. It includes and extends the practices of information security incident handling and management and ICT readiness planning and services.	
149.	ISO/IEC JTC 1/SC 27 , Information security, cybersecurity and privacy protection	ISO/IEC 27035-1, Information technology — Security techniques — Information security incident management — Part 1: Principles of incident management	published	ISO/IEC 27035-1:2016 is the foundation of this multipart International Standard. It presents basic concepts and phases of information security incident management and combines these concepts with principles in a structured approach to detecting, reporting, assessing, and responding to incidents, and applying lessons learnt. The principles given in ISO/IEC 27035-1:2016 are generic and intended to be applicable to all organizations, regardless of type, size or nature. Organizations can adjust the guidance given in ISO/IEC 27035-1:2016 according to their type, size and nature of business in relation to the information security risk situation. It is also applicable to external organizations providing information security incident management services.	

	Standardization Body	Title	Status	Summary	CitySCAPE Action
150.	ISO/IEC JTC 1/SC 27 , Information security, cybersecurity and privacy protection	ISO/IEC 27035-2, Information technology — Security techniques — Information security incident management — Part 2: Guidelines to plan and prepare for incident response	published	<p>ISO/IEC 27035-2:2016 provides the guidelines to plan and prepare for incident response. The guidelines are based on the "Plan and Prepare" phase and the "Lessons Learned" phase of the "Information security incident management phases" model presented in ISO/IEC 27035-1.</p> <p>The major points within the "Plan and Prepare" phase include the following:</p> <ul style="list-style-type: none"> - information security incident management policy and commitment of top management; - information security policies, including those relating to risk management, updated at both corporate level and system, service and network levels; - information security incident management plan; - incident response team (IRT) establishment; - establish relationships and connections with internal and external organizations; - technical and other support (including organizational and operational support); - information security incident management awareness briefings and training; - information security incident management plan testing. <p>The principles given in this part of ISO/IEC 27035 are generic and intended to be applicable to all organizations, regardless of type, size or nature. Organizations can adjust the guidance given in this part of ISO/IEC 27035 according to their type, size and nature of business in relation to the information security risk situation. This part of ISO/IEC 27035 is also applicable to external organizations providing information security incident management services.</p>	

	Standardization Body	Title	Status	Summary	CitySCAPE Action
151.	ISO/IEC JTC 1/SC 27 , Information security, cybersecurity and privacy protection	ISO/IEC 27035-3, Information technology — Information security incident management — Part 3: Guidelines for ICT incident response operations	published	<p>This document gives guidelines for information security incident response in ICT security operations. This document does this by firstly covering the operational aspects in ICT security operations from a people, processes and technology perspective. It then further focuses on information security incident response in ICT security operations including information security incident detection, reporting, triage, analysis, response, containment, eradication, recovery and conclusion.</p> <p>This document is not concerned with non-ICT incident response operations such as loss of paper-based documents.</p> <p>This document is based on the "Detection and reporting" phase, the "Assessment and decision" phase and the "Responses" phase of the "Information security incident management phases" model presented in ISO/IEC 27035-1:2016.</p> <p>The principles given in this document are generic and intended to be applicable to all organizations, regardless of type, size or nature. Organizations can adjust the provisions given in this document according to their type, size and nature of business in relation to the information security risk situation.</p> <p>This document is also applicable to external organizations providing information security incident management services.</p>	
152.	ISO/IEC JTC 1/SC 27 , Information security, cybersecurity and privacy protection	ISO/IEC 27039:2015 , Information technology — Security techniques — Selection, deployment and operations of intrusion detection and prevention systems (IDPS)	Published	<p>ISO/IEC 27039:2015 provides guidelines to assist organizations in preparing to deploy intrusion detection and prevention systems (IDPS). In particular, it addresses the selection, deployment, and operations of IDPS. It also provides background information from which these guidelines are derived.</p>	ENG will apply this standard in T5.4 for the development of CITYSCAPE IDS/IPS

	Standardization Body	Title	Status	Summary	CitySCAPE Action
153.	ISO/IEC JTC 1/SC 27 , Information security, cybersecurity and privacy protection	ISO/IEC 15408-1:2009 , Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model	published	<p>ISO/IEC 15408-1:2009 establishes the general concepts and principles of IT security evaluation and specifies the general model of evaluation given by various parts of ISO/IEC 15408 which in its entirety is meant to be used as the basis for evaluation of security properties of IT products.</p> <p>It provides an overview of all parts of ISO/IEC 15408. It describes the various parts of ISO/IEC 15408; defines the terms and abbreviations to be used in all parts ISO/IEC 15408; establishes the core concept of a Target of Evaluation (TOE); the evaluation context; and describes the audience to which the evaluation criteria are addressed. An introduction to the basic security concepts necessary for evaluation of IT products is given.</p> <p>It defines the various operations by which the functional and assurance components given in ISO/IEC 15408-2 and ISO/IEC 15408-3 may be tailored through the use of permitted operations. The key concepts of protection profiles (PP), packages of security requirements and the topic of conformance are specified and the consequences of evaluation and evaluation results are described. ISO/IEC 15408-1:2009 gives guidelines for the specification of Security Targets (ST) and provides a description of the organization of components throughout the model.</p> <p>General information about the evaluation methodology is given in ISO/IEC 18045 and the scope of evaluation schemes is provided.</p>	CSG: T8.2 is taken into account this standard in order to check if it should be taken into account as part of the labelling process to be defined.
154.	ISO/IEC JTC 1/SC 27 , Information security, cybersecurity and privacy protection	ISO/IEC 15408-2:2008 , Information technology — Security techniques — Evaluation criteria for IT security — Part 2: Security functional components	published	<p>Defines the required structure and content of security functional components for the purpose of security evaluation. It includes a catalogue of functional components that will meet the common security functionality requirements of many IT products.</p>	CSG: T8.2 is taken into account this standard in order to check if it should be taken into account as part of the labelling process to be defined.
155.	ISO/IEC JTC 1/SC 27 , Information security, cybersecurity and privacy protection	ISO/IEC 15408-3:2008 , Information technology — Security techniques — Evaluation criteria for IT security — Part 3: Security assurance components	published	<p>Defines the assurance requirements of ISO/IEC 15408. Includes the evaluation assurance levels (EALs) that define a scale for measuring assurance for component Targets of Evaluation (TOEs), the composed assurance packages (CAPs) that define a scale for measuring assurance for composed TOEs, the individual assurance components from which the assurance levels and packages are composed, and the criteria for evaluation of Protection Profiles (PPs) and Security Targets (STs).</p>	CSG: T8.2 is taken into account this standard in order to check if it should be taken into account as part of the labelling process to be defined.

	Standardization Body	Title	Status	Summary	CitySCAPE Action
156.	ISO/IEC JTC 1/SC 27 , Information security, cybersecurity and privacy protection	ISO/IEC 15408-4:2022 , Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 4: Framework for the specification of evaluation methods and activities	published	Describes a framework that can be used for deriving Evaluation Activities from work units of ISO/IEC 18045 and grouping them into 'Evaluation Methods'.	CSG: T8.2 is taken into account this standard in order to check if it should be taken into account as part of the labelling process to be defined.
157.	ISO/IEC JTC 1/SC 27 , Information security, cybersecurity and privacy protection	ISO/IEC 15408-5:2022 , Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 5: Pre-defined packages of security requirements	published	Provides packages of security assurance and security functional requirements that have been identified as useful in support of common usage by stakeholders (f.e. evaluation assurance levels (EAL) and the composed assurance packages (CAPs)).	CSG: T8.2 is taken into account this standard in order to check if it should be taken into account as part of the labelling process to be defined.
158.	ISO/IEC JTC 1/SC 27 , Information security, cybersecurity and privacy protection	ISO/IEC 18045:2022 , Information technology — Security techniques — Methodology for IT security evaluation	published	Represents a companion document to the evaluation criteria for IT security defined in ISO/IEC 15408. Defines the minimum actions to be performed by an evaluator in order to conduct an ISO/IEC 15408 evaluation, using the criteria and evaluation evidence defined in ISO/IEC 15408.	CSG: T8.2 is taken into account this standard in order to check if it should be taken into account as part of the labelling process to be defined.
159.	ISO/IEC JTC 1/SC 27 , Information security, cybersecurity and privacy protection	ISO/IEC TS 19608:2018, Guidance for developing security and privacy functional requirements based on ISO/IEC 15408	published	Provides guidance for: <ul style="list-style-type: none"> - selecting and specifying security functional requirements (SFRs) from ISO/IEC 15408-2 to protect Personally Identifiable Information (PII); - the procedure to define both privacy and security functional requirements in a coordinated manner; and - developing privacy functional requirements as extended components based on the privacy principles defined in ISO/IEC 29100 through the paradigm described in ISO/IEC 15408-2. 	
160.	ISO/IEC JTC 1/SC 27 , Information security, cybersecurity and privacy protection	ISO/IEC TR 20004:2015, Information technology — Security techniques — Refining software vulnerability analysis under ISO/IEC 15408 and ISO/IEC 18045	published	Provide added refinement, detail and guidance to the vulnerability analysis activities outlined in ISO/IEC 18045:2008 for the software elements of a TOE. Specifically, it is intended to add refinement and clarification of the “Potential vulnerability identification from public sources” (AVA_VAN.1.2E/2.2E/3.2E/4.2E) and “Penetration testing” (AVA_VAN.1.3E/2.4E/3.4E/4.4E) evaluator actions.	

	Standardization Body	Title	Status	Summary	CitySCAPE Action
161.	ISO/IEC JTC 1/SC 27 , Information security, cybersecurity and privacy protection	ISO/IEC 30111:2019 , Information technology — Security techniques — Vulnerability handling processes	published	This document provides requirements and recommendations for how to process and remediate reported potential vulnerabilities in a product or service. This document is applicable to vendors involved in handling vulnerabilities.	
162.	ISO/IEC JTC 1/SC 37 Biometrics	ISO/IEC 19794 Information technology — Biometric data interchange formats (series of standards)	published	This series of standards describes interchange formats for several types of biometric data.	
163.	ISO/IEC JTC 1/SC 38 Cloud computing and distributed platforms	ISO/IEC 17788:2014 , Information technology — Cloud computing — Overview and vocabulary	published	ISO/IEC 17788:2014 provides an overview of cloud computing along with a set of terms and definitions. It is a terminology foundation for cloud computing standards. ISO/IEC 17788:2014 is applicable to all types of organizations (e.g., commercial enterprises, government agencies, not-for-profit organizations).	
164.	ISO/IEC JTC 1/SC 41 , Internet of things and digital twin	ISO/IEC 21823-1:2019 Internet of things (IoT) — Interoperability for IoT systems — Part 1: Framework	published	ISO/IEC 21823-1:2019(E) provides an overview of interoperability as it applies to IoT systems and a framework for interoperability for IoT systems. This document enables IoT systems to be built in such a way that the entities of the IoT system are able to exchange information and mutually use the information in an efficient way. This document enables peer-to-peer interoperability between separate IoT systems. This document provides a common understanding of interoperability as it applies to IoT systems and the various entities within them.	
165.	ISO/IEC JTC 1/SC 41 , Internet of things and digital twin	ISO/IEC 21823-2:2020 Internet of things (IoT) — Interoperability for IoT systems — Part 2: Transport interoperability	published	ISO/IEC 21823-2:2020(E) specifies a framework and requirements for transport interoperability, in order to enable the construction of IoT systems with information exchange, peer-to-peer connectivity and seamless communication both between different IoT systems and also among entities within an IoT system. This document specifies: <ul style="list-style-type: none"> - transport interoperability interfaces and requirements between IoT systems; - transport interoperability interfaces and requirements within an IoT system 	

	Standardization Body	Title	Status	Summary	CitySCAPE Action
166.	ISO/IEC JTC 1/SC 41 , Internet of things and digital twin	ISO/IEC 30141:2018 Internet of Things (IoT) — Reference Architecture	published	ISO/IEC 30141:2018 This document provides a standardized IoT Reference Architecture using a common vocabulary, reusable designs and industry best practices. It uses a top-down approach, beginning with collecting the most important characteristics of IoT, abstracting those into a generic IoT Conceptual Model, deriving a high level system based reference with subsequent dissection of that model into five architecture views from different perspectives.	
167.	CEN/CENELEC JTC 13 , Cybersecurity and Data Protection	prCEN/TR Data protection and privacy by design and by default - Technical Report on applicability to the video surveillance industry - State of the art	under development	This document contains recommendations on how to integrate the principle of 'data protection and privacy by design' during the entire lifecycle of video-surveillance products and services, in order to achieve 'data protection and privacy by default'.	
168.	CEN/CENELEC JTC 13 , Cybersecurity and Data Protection	prCEN/TR 2 Privacy management in products and services - Biometric access control products and services	under development	This document contains recommendations on how to integrate the principle of 'data protection and privacy by design' during the entire lifecycle of biometric access-control products and services, in order to achieve 'data protection and privacy by default'. Biometric facial recognition for access control is covered by this document. Biometric facial recognition for surveillance is covered by CEN/CLC/JTC 13 TR 'Video surveillance'. This document specifies recommendations for the management of data protection and privacy by design in biometric access-control products and services. This document extends ISO/IEC 27552. This document applies to aspects of data protection and privacy by design. This document is not applicable to non-biometric aspects of access control, or to aspects not relating to data protection or privacy.	
169.	CEN/CENELEC JTC 13 , Cybersecurity and Data Protection	EN 17529:2022 Data protection and privacy by design and by default	published	This EN contains requirements for manufacturers and / or service providers to consider data protection and data security aspects early in the development process of their products and services and to implement them as a basic setting. This standard will be applicable to all sectors including the security industry.	

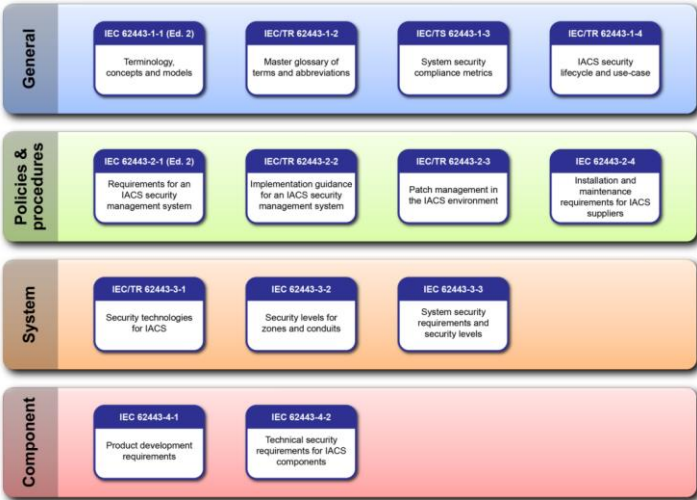
	Standardization Body	Title	Status	Summary	CitySCAPE Action
170.	CEN/CENELEC JTC 13 , Cybersecurity and Data Protection	prEN 17640 Fixed time cybersecurity evaluation methodology for ICT products	under development	This document describes the cybersecurity evaluation methodology for ICT products. It is intended for use for all three assurance levels as defined in the Cybersecurity Act (i.e. basic, substantial and high). The methodology is comprised of different evaluation blocks including assessment activities that comply with the evaluation requirements of the CSA for the three levels. Where appropriate, it can be applied both to 3rd party evaluation and self-assessment. It is expected that this methodology may be used by different candidate schemes and verticals providing a common framework to evaluate ICT products.	
171.	ISO/TMBG Technical Management Board - groups	IWA 14-2:2013 , Vehicle security barriers — Part 2: Application	published	Provides guidance for the selection, installation and use of vehicle security barriers (VSBs) and describes the process of producing operational requirements (ORs).	
172.	NIST	Advanced Encryption Standard (AES 256)	published	Specifies a FIPS-approved cryptographic algorithm for protection of electronic data using cryptographic keys of 256 bits.	KSP: The MobSec mobile App defined in Task 3.3 and implemented by SIGLA to build a 'secure by design' mobile app for passengers of multimodal local transport is integrated with Kaspersky Mobile Security SDK (KMS-SDK). KMS-SDK encrypts internal product data files and security requests to KSN following AES 256 Data Encryption Standard

	Standardization Body	Title	Status	Summary	CitySCAPE Action
173.	NIST	SP 800-53 Rev. 5: 2020, Security and Privacy Controls for Information Systems and Organizations	published	This publication provides a catalogue of security and privacy controls for information systems and organizations to protect organizational operations and assets, individuals, other organizations, and the Nation from a diverse set of threats and risks, including hostile attacks, human errors, natural disasters, structural failures, foreign intelligence entities, and privacy risks. The controls are flexible and customizable and implemented as part of an organization-wide process to manage risk. The controls address diverse requirements derived from mission and business needs, laws, executive orders, directives, regulations, policies, standards, and guidelines. Finally, the consolidated control catalogue addresses security and privacy from a functionality perspective (i.e., the strength of functions and mechanisms provided by the controls) and from an assurance perspective (i.e., the measure of confidence in the security or privacy capability provided by the controls). Addressing functionality and assurance helps to ensure that information technology products and the systems that rely on those products are sufficiently trustworthy.	
174.	IEEE	IEEE 1609.0-2019 - IEEE Guide for Wireless Access in Vehicular Environments (WAVE) Architecture	published	Describes the wireless access in vehicular environments (WAVE) architecture and services necessary for WAVE devices to communicate in a mobile vehicular environment.	
175.	IEEE	IEEE 1609.2-2016 - IEEE Standard for Wireless Access in Vehicular Environments--Security Services for Applications and Management Messages	published	Defines secure message formats and processing for use by Wireless Access in Vehicular Environments (WAVE) devices, including methods to secure WAVE management messages and methods to secure application messages. It also describes administrative functions necessary to support the core security functions.	
176.	IEEE	IEEE 1609.3-2016 - IEEE Standard for Wireless Access in Vehicular Environments (WAVE) -- Networking Services	published	Describes services to WAVE devices and systems are provided in IEEE Std 1609.3(TM), IEEE Standard for Wireless Access in Vehicular Environments (WAVE)—Networking Services. Layer 3 and layer 4 of the open system interconnect (OSI) model and the Internet Protocol (IP), User Datagram Protocol (UDP), and Transmission Control Protocol (TCP) elements of the Internet model.	
177.	IEEE	IEEE 1609.4-2016 - IEEE Standard for Wireless Access in Vehicular Environments (WAVE) -- Multi-Channel Operation	published	Describes multi-channel wireless radio operations, Wireless Access in Vehicular Environments (WAVE) mode, medium access control (MAC), and physical layers (PHYs), including parameters for priority access, channel switching and routing, management services, and primitives designed for multi-channel operations.	

	Standardization Body	Title	Status	Summary	CitySCAPE Action
178.	IEEE	IEEE 1609.11-2010 - IEEE Standard for Wireless Access in Vehicular Environments (WAVE)-- Over-the-Air Electronic Payment Data Exchange Protocol for Intelligent Transportation Systems (ITS)	published	Specifies the electronic payment service layer and profile for Payment and Identity authentication, and Payment Data transfer for Dedicated Short-Range Communication (DSRC) based applications in Wireless Access in Vehicular Environments.	
179.	IEEE	IEEE 1609.12-2019 - IEEE Standard for Wireless Access in Vehicular Environments (WAVE)-- Identifiers	published	Indicates the identifiers within Wireless Access in Vehicular Environments (WAVE).	
180.	IEEE	IEEE 802-2014 - IEEE Standard for Local and Metropolitan Area Networks: Overview and Architecture	published	Provides an overview to the family of IEEE 802® standards. It describes the reference models for the IEEE 802 standards and explains the relationship of these standards to the higher layer protocols; it provides a standard for the structure of IEEE 802 MAC addresses; it provides a standard for identification of public, private, prototype, and standard protocols; it specifies an object identifier hierarchy used within IEEE 802 for uniform allocation of object identifiers used in IEEE 802 standards; and it specifies a method for higher layer protocol identification. More information on the group of standards: https://ieeexplore.ieee.org/browse/standards/get-program/page/series?id=68	
181.	IEEE	IEEE/ISO/IEC 8802-2-1998 - ISO/IEC/IEEE International Standard for Information technology -- Telecommunications and information exchange between systems -- Local and metropolitan area networks -- Specific requirements -- Part 2: Logical Link Control	published	Describes the functions, features, protocol, and services of the Logical Link Control (LLC) sublayer, which constitutes the top sublayer in the data link layer of the ISO/IEC 8802 LAN protocol.	

	Standardization Body	Title	Status	Summary	CitySCAPE Action
182.	IEEE	IEEE/ISO/IEC 8802-3-2014 - ISO/IEC/IEEE International Standard for Ethernet	published	Specifies Ethernet local area network operation for selected speeds of operation from 1 Mb/s to 100 Gb/s using a common media access control (MAC) specification and management information base (MIB).	
183.	IEC TC 9 - Electrical equipment and systems for railways	IEC 61375 Electronic railway equipment - Train communication network (TCN) (series)	published	The series of the standard covers the TCN components, used in most of the modern train control systems	
184.	IEC TC 9 - Electrical equipment and systems for railways	IEC 61991:2019 RLV Railway applications - Rolling stock - Protective provisions against electrical hazards	published	Defines requirements applied in the design and manufacture of electrical installations and equipment to be used on rolling stock to protect persons from electric shocks.	
185.	IEC TC 9 - Electrical equipment and systems for railways	IEC 62267:2009 Railway applications - Automated urban-guided transport (AUGT) - Safety requirements	published	IEC 62267:2009 covers high-level safety requirements applicable to automated urban guided transport systems, with driverless or unattended self-propelled trains, operating on an exclusive guideway. Deals with the safety requirements needed to compensate for the absence of a driver or attendant staff who would otherwise be responsible for some or all of train operation functions, depending on the level of automation of the system.	
186.	IEC TC 9 - Electrical equipment and systems for railways	IEC TR 62267-2:2011 Railway applications - Automated urban guided transport (AUGT) - Safety requirements - Part 2: Hazard analysis at top system level	published	IEC/TR 62267-2:2011(E) provides a non-normative generic hazard analysis at top system level conducted for the development of IEC 62267 for Automated Urban Guided Transport (AUGT) systems. This report is applicable to all systems covered by the scope of IEC 62267. This generic hazard analysis can be used for specific AUGT systems to support the necessary activities in lifecycle process following IEC 62278.	
187.	IEC TC 9 - Electrical equipment and systems for railways	IEC 62279:2015 Railway applications - Communication, signalling and processing systems - Software for railway control and protection systems	published	Specifies the process and technical requirements for the development of software for programmable electronic systems for use in railway control and protection applications.	

	Standardization Body	Title	Status	Summary	CitySCAPE Action
188.	IEC TC 9 - Electrical equipment and systems for railways	IEC 62280:2014 Railway applications - Communication, signalling and processing systems - Safety related communication in transmission systems	published	Gives the basic requirements needed to achieve safety related communication between safety related equipment connected to the transmission system.	
189.	IEC TC 9 - Electrical equipment and systems for railways	IEC 62290-1:2014 Railway applications - Urban guided transport management and command/control systems - Part 1: System principles and fundamental concepts	published	Provides an introduction to the standard and deals with the main concepts, the system definition, the principles and the basic functions of UGTMSs (Urban Guided Transport Management and Command/Control Systems) for use in urban guided passenger transport lines and networks.	
190.	IEC TC 9 - Electrical equipment and systems for railways	IEC 62290-2:2014 Railway applications - Urban guided transport management and command/control systems - Part 2: Functional requirements specification	published	Specifies the functional requirements of UGTMSs (Urban Guided Transport Management and Command/Control Systems) for use in urban guided passenger transport lines and networks.	
191.	IEC TC 9 - Electrical equipment and systems for railways	IEC 62290-3:2019 Railway applications - Urban guided transport management and command/control systems - Part 3: System requirements specification	published	Specifies the system architecture for Urban Guided Transport Management and Command/Control systems (UGTMS) as defined in IEC 62290-1 and IEC 62290-2, and the allocation of functions and requirements defined in IEC 62290-2 to the different UGTMS subsystems (designated as system constituents in IEC 62290-1 and IEC 62290-2), for use in urban guided passenger transport lines and networks.	
192.	IEC TC 9 - Electrical equipment and systems for railways	IEC 62580-1:2015 Electronic railway equipment - On-board multimedia and telematic subsystems for railways - Part 1: General architecture	published	IEC 62580-1:2015 specifies the general architecture of the On-board Multimedia and Telematic Subsystem (OMTS)	
193.	IEC TC 9 - Electrical equipment and systems for railways	IEC TS 62580-2:2016 Electronic railway equipment - On-board multimedia and telematic subsystems for railways - Part 2: Video surveillance/CCTV services	published	IEC TS 62580-2:2016(E) specifies the on-board video surveillance/CCTV system functionality and requirement for the purpose of interoperability between components of on-board video surveillance/CCTV systems in the same vehicle and subsystems in different vehicles of the same train, which means two levels of interoperability are considered, one is interoperability between components, and another is between subsystems.	

	Standardization Body	Title	Status	Summary	CitySCAPE Action
194.	IEC TC 65, Industrial-process measurement, control and automation	IEC TS 62443-1-1:2009 Industrial communication networks - Network and system security - Part 1-1: Terminology, concepts and models	published	<p>This multi-part standard is divided into different sections and describes both technical and process-related aspects of industrial cybersecurity. It divides the industry into different roles: the operator, the integrators (service providers for integration and maintenance) and the manufacturers. The different roles each follow a risk-based approach to prevent and manage security risks in their activities.</p>  <p>IEC 62443 describes different levels of maturity for processes and technical requirements. The maturity levels for processes are based on the maturity levels from the CMMI framework.</p> <p>Maturity Level: IEC 62443 describes different maturity levels for processes through so-called "maturity levels". To fulfil a certain level of a maturity level, all process-related requirements must always be practiced during product development or integration, i.e. the selection of only individual criteria ("cherry picking") is not standard-compliant.</p> <p>The maturity levels are described as follows:</p>	

	Standardization Body	Title	Status	Summary	CitySCAPE Action
				<p>Maturity Level 1 - Initial: Product suppliers usually carry out product development ad hoc and often undocumented (or not fully documented).</p> <p>Maturity Level 2 - Managed: The product supplier is able to manage the development of a product according to written guidelines. It must be demonstrated that the personnel who carry out the process have the appropriate expertise, are trained and/or follow written procedures. The processes are repeatable.</p> <p>Maturity Level 3 - Defined (practiced): The process is repeatable throughout the supplier's organization. The processes have been practiced and there is evidence that this has been done.</p> <p>Maturity Level 4 - Improving: Product suppliers use appropriate process metrics to monitor the effectiveness and performance of the process and demonstrate continuous improvement in these areas.</p> <p>Security Level</p> <p>Technical requirements for systems (IEC 62443-3-3) and products (IEC 62443-4-2) are evaluated in the standard by four so-called Security Levels (SL). The different levels indicate the resistance against different classes of attackers. The standard emphasizes that the levels should be evaluated per technical requirement (see IEC 62443-1-1) and are not suitable for the general classification of products.</p> <p>The levels are:</p> <p>Security Level 0: No special requirement or protection required.</p> <p>Security Level 1: Protection against unintentional or accidental misuse.</p> <p>Security Level 2: Protection against intentional misuse by simple means with few resources, general skills and low motivation.</p> <p>Security Level 3: Protection against intentional misuse by sophisticated means with moderate resources, IACS-specific knowledge and moderate motivation.</p> <p>Security Level 4: Protection against intentional misuse using sophisticated means with extensive resources, IACS-specific knowledge and high motivation.</p>	

	Standardization Body	Title	Status	Summary	CitySCAPE Action
				<p>Concepts: The standard explains various basic principles that should be considered for all roles in all activities.</p> <p>Defense in Depth is a concept in which several levels of security (defense) are distributed throughout the system. The goal is to provide redundancy in case a security measure fails, or a vulnerability is exploited.</p> <p>Zones & Conduits: Zones divide a system into homogeneous zones by grouping the (logical or physical) assets with common security requirements. The security requirements are defined by Security Level (SL). The level required for a zone is determined by the risk analysis. Zones have boundaries that separate the elements inside the zone from those outside. Information moves within and between zones. Zones can be divided into sub-zones that define different security levels (Security Level) and thus enable defence-in-depth. Conduits group the elements that allow communication between two zones. They provide security functions that enable secure communication and allow the coexistence of zones with different security levels.</p>	
195.	IEC TC 65 , Industrial- process measurement, control and automation	IEC 62443-2-1:2010 Industrial communication networks - Network and system security - Part 2-1: Establishing an industrial automation and control system security program	published	Defines the elements necessary to establish a cyber security management system (CSMS) for industrial automation and control systems (IACS) and provides guidance on how to develop those elements.	
196.	IEC TC 65 , Industrial- process measurement, control and automation	IEC TR 62443-2-3:2015 Security for industrial automation and control systems - Part 2-3: Patch management in the IACS environment	published	Describes requirements for asset owners and industrial automation and control system (IACS) product suppliers that have established and are now maintaining an IACS patch management program.	

	Standardization Body	Title	Status	Summary	CitySCAPE Action
197.	IEC TC 65 , Industrial-process measurement, control and automation	IEC 62443-2-4:2015+AMD1:2017 CSV Security for industrial automation and control systems - Part 2-4: Security program requirements for IACS service providers	published	Specifies requirements for security capabilities for IACS service providers that they can offer to the asset owner during integration and maintenance activities of an Automation Solution. This consolidated version consists of the first edition (2015) and its amendment 1 (2017).	
198.	IEC TC 65 , Industrial-process measurement, control and automation	IEC TR 62443-3-1:2009 Industrial communication networks - Network and system security - Part 3-1: Security technologies for industrial automation and control systems	published	Provides a current assessment of various cybersecurity tools, mitigation countermeasures, and technologies that may effectively apply to the modern electronically based IACSS regulating and monitoring numerous industries and critical infrastructures.	
199.	IEC TC 65 , Industrial-process measurement, control and automation	IEC 62443-3-2:2020 Security for industrial automation and control systems - Part 3-2: Security risk assessment for system design	published	Establishes requirements for: <ul style="list-style-type: none"> • defining a system under consideration (SUC) for an industrial automation and control system (IACS); • partitioning the SUC into zones and conduits; • assessing risk for each zone and conduit; • establishing the target security level (SL-T) for each zone and conduit; and • documenting the security requirements. 	
200.	IEC TC 65 , Industrial-process measurement, control and automation	IEC 62443-3-3:2013 Industrial communication networks - Network and system security - Part 3-3: System security requirements and security levels	published	Provides detailed technical control system requirements (SRs) associated with the seven foundational requirements (FRs) described in IEC 62443-1-1 including defining the requirements for control system capability security levels, SL-C (control system).	
201.	IEC TC 65 , Industrial-process measurement, control and automation	IEC 62443-4-1:2018 Security for industrial automation and control systems - Part 4-1: Secure product development lifecycle requirements	published	Specifies the process requirements for the secure development of products used in industrial automation and control systems.	

	Standardization Body	Title	Status	Summary	CitySCAPE Action
202.	IEC TC 65 , Industrial-process measurement, control and automation	IEC 62443-4-2:2019 Security for industrial automation and control systems - Part 4-2: Technical security requirements for IACS components	published	Provides detailed technical control system component requirements (CRs) associated with the seven foundational requirements (FRs) described in IEC TS 62443-1-1 including defining the requirements for control system capability security levels and their components, SL-C(component).	
203.	IEC TC 65 , Industrial-process measurement, control and automation	IEC TR 63074:2019 Safety of machinery - Security aspects related to functional safety of safety-related control systems	published	Gives guidance on the use of IEC 62443 (all parts) related to those aspects of security threats and vulnerabilities that could influence functional safety implemented and realized by safety-related control systems (SCS) and could lead to the loss of the ability to maintain safe operation of a machine.	
204.	IEC TC 79 - Alarm and electronic security systems	IEC 60839-10-1:1995 Alarm systems - Part 10: Alarm systems for road vehicles - Section 1: Passenger cars	published	Specifies requirements and test methods for vehicle security alarm systems intended for installation within vehicles used for the carriage of passengers and having not more than eight seats in addition to the driver's seat.	
205.	IEC TC 79 - Alarm and electronic security systems	IEC 62642-8:2011 Alarm systems - Intrusion and hold-up systems - Part 8: Security fog device/systems	published	Specifies the requirements for security fog systems as a part of an I&HAS. It covers application and performance and also gives the necessary tests and trials to ensure efficiency and reliability of such obscuration devices. It also gives guidance on the criteria for design, installation, operation and maintenance of security fog systems.	
206.	IEC TC 79 - Alarm and electronic security systems	IEC 62676 Video surveillance systems for use in security applications (series)	published	This series of standards specifies the requirements and gives recommendations for Video Surveillance Systems (VSS), installed for security applications.	
207.	ETSI TC ITS Intelligent Transport Systems	ETSI EN 302 890-2 V2.1.1 (2020-10) Intelligent Transport Systems (ITS); Facilities Layer function; Part 2: Position and Time management (PoTi); Release 2	published	European Norm of the position & time function according to functional and operational requirements of supported applications.	

	Standardization Body	Title	Status	Summary	CitySCAPE Action
208.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 103 601 V1.1.1 (2020-10) Intelligent Transport Systems (ITS); Security; Security management messages communication requirements and distribution protocols	published	The deliverable will define communication requirements and profiles to support communications from/to ITS-S stations (e.g. fixed road side ITS-S, mobile ITS-S) for the support of security management services specified in TS 102 941 (i.e. certificate management, trust and revocation lists distribution). The deliverable will also define the related protocol handling for the selected messages as well as the requirements for the lower layer protocol stacks and for the security processing services sub-entity in order to support message dissemination and reception.	
209.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 103 097 V1.4.1 (2020-10) Intelligent Transport Systems (ITS); Security; Security header and certificate formats	published	To revise TS 103 097 in Release1 following the issues raised from ETSI ITS CMS#7 Plugtests and required corrections impacting the deployment of the EU CCMS. To apply CR#1 on the HeaderInfo extensibility mechanism and CR#2 on HeaderFields extensions to support TS 103 601 Peer2Peer distributions.	
210.	ETSI TC ITS Intelligent Transport Systems	ETSI TR 103 496 V2.1.1 (2020-10) Intelligent Transport Systems (ITS); Cooperative ITS (C-ITS) support for transport pollution management applications; Use cases and standardization study; Release 2	published	To study how C-ITS architecture and V2X communication technology could be used to enable new type of transport pollution control and management applications. Based on the identification and analysis of major use cases, the document will provide a recommendation for the extension of the existing ETSI ITS standards with new ITS applications reducing the environmental transport impact and improving the transport pollution control. The document will also include use cases desired by road operators.	
211.	ETSI TC ITS Intelligent Transport Systems	ETSI TR 103 460 V2.1.1 (2020-10) Intelligent Transport Systems (ITS); Security; Pre-standardization study on Misbehavior Detection; Release 2	published	to realize an overview of the relevant misbehavior detection and mechanisms suitable for C-ITS and provide a comparison of the performances of different misbehavior detection mechanisms. Moreover, the deliverable will provide the potential minimum requirements of security architecture and misbehavior detection distribution mechanisms	

	Standardization Body	Title	Status	Summary	CitySCAPE Action
212.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 103 723 V1.1.1 (2020-09) Intelligent Transport Systems (ITS); Profile for LTE-V2X Direct Communication	published	<p>To identify a common set of standards and specify configuration parameter values and references required for the implementation of direct communication between ITS stations, to achieve interoperable deployment of ITS services via V2V and V2I links. The scope is limited to LTE-V2X mode 4. Additional requirements like triggering conditions, position accuracy, security, and functional safety aspects are out of scope. Descriptions, definitions and rules for all layers (Applications, Facilities, Networking & Transport and Access) of the ETSI ITS station reference architecture will be considered.</p> <p>The scope is limited to communication aspects of ITS stations using a single access layer technology (i.e., LTE-V2X). Additional requirements like triggering conditions, position accuracy, security, and functional safety aspects are out of scope. Descriptions, definitions and rules for all layers (Applications, Facilities, Networking & Transport and Access) of the ETSI ITS station reference architecture will be considered.</p>	
213.	ETSI TC ITS Intelligent Transport Systems	ETSI TR 103 579 V1.1.1 (2020-09) Intelligent Transport Systems (ITS); Pre-Standardization Study on payment applications in Cooperative ITS using V2I communication	published	Identify potential requirements for the set of payment applications including positioning and security requirements. To investigate possible updates and changes to the existing set of ETSI Cooperative ITS standards using V2I communication, to support locally hosted payment applications including Electronic Fee Collection (EFC) and other general payment applications.	

	Standardization Body	Title	Status	Summary	CitySCAPE Action
214.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 102 165-1 V5.2.5 (2022-01), CYBER; Methods and protocols; Part 1: Method and pro forma for Threat, Vulnerability, Risk Analysis (TVRA)	published	<p>The present document defines a method primarily for use by ETSI standards developers in undertaking an analysis of the threats, risks and vulnerabilities of an Information and Communications Technology (ICT) system.</p> <p>NOTE: The method described has been tailored to apply to pre-production but can be applied to production devices with due attention given to possibility that the application of countermeasures may be unachievable for a re-design strategy.</p> <p>The method described in the present document builds from the Common Criteria for security assurance and evaluation defined in ISO/IEC 15408 [i.27], [i.28], [i.29] and specifically targets the means to build a Threat Vulnerability and Risk Analysis (TVRA) to allow its reference by an ETSI specification developed using the guidelines given in ETSI EG 202 387 [i.1] and ETSI ES 202 382 [i.24]. The TVRA forms part of the documentation set for the Target Of Evaluation as specified in ETSI ES 202 382 [i.24] with its intended audience being a developer of standards based Protection Profiles.</p> <p>The use of the method described in the present document for application outside the "Design for Assurance" paradigm described in ETSI EG 202 387 [i.1] is supported but some of the examples and stages of evaluation may not be appropriate.</p>	
215.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 102 636-4-3 V1.1.1 (2020-08) Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 4: Geographical addressing and forwarding for point-to-point and point-to-multipoint communications; Sub-part 3: Media-dependent functionalities for LTE-V2X	published	<p>Added those LTE-V2X specific statements that had to be removed from EN 302 636-4-1 GeoNetworking media-independent, specifically:</p> <ul style="list-style-type: none"> - Fields of the GeoNetworking address, - Overall packet structure for LTE-V2X access layer technology, - Packet handling. <p>Aligned the deliverable to changes in EN 302 613 (LTE-V2X access layer) and TS 103 574 (Congestion Control).</p>	

	Standardization Body	Title	Status	Summary	CitySCAPE Action
216.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 102 636-4-2 V1.3.1 (2020-08) Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 4: Geographical addressing and forwarding for point-to-point and point-to-multipoint communications; Sub-part 2: Media-dependent functionalities for ITS-G5	published	Corrections: 1. Contradicting statements: Is DCC mandatory for GeoNetworking over ITS-G5? 2. DCC for ITS-S operating in the ITS G5 band 3. DCC_CROSS_Net	
217.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 103 300-2 V2.1.1 (2020-05) Intelligent Transport System (ITS); Vulnerable Road Users (VRU) awareness; Part 2: Functional Architecture and Requirements definition; Release 2	published	The Technical Specification defines the VRU related requirements (stage 2); as well as the functional architecture of the VRU system (stage 3). In addition, it analyses the impact on existing standards (for instance the CAM European Standard)	
218.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 102 636-4-2 V1.2.1 (2020-04) Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 4: Geographical addressing and forwarding for point-to-point and point-to-multipoint communications; Sub-part 2: Media-dependent functionalities for ITS-G5	published	Add those ITS-G5 specific statements that had to be removed from EN 302 636-4-1 GeoNetworking media-independent, specifically: - Fields of the GeoNetworking address, - Overall packet structure for ITS-G5 access layer technology, - Packet handling. Align the deliverable to changes in EN 302 663 (ITS G5 access layer) and TS 103 175 (Crosslayer DCC).	

	Standardization Body	Title	Status	Summary	CitySCAPE Action
219.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 102 868-1 V1.5.1 (2020-04) Intelligent Transport Systems (ITS); Testing; Conformance test specifications for Cooperative Awareness Basic Service (CA); Part 1: Test requirements and Protocol Implementation Conformance Statement (PICS) pro forma	published	To update CAM test specification to align with the latest version of EN 302 637-2 and TS 103 097	
220.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 102 868-2 V1.5.1 (2020-04) Intelligent Transport Systems (ITS); Testing; Conformance test specifications for Cooperative Awareness Basic Service (CA); Part 2: Test Suite Structure and Test Purposes (TSS & TP)	published	Update according to feedback from Validation and CDD changes.	
221.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 102 868-3 V1.5.1 (2020-04) Intelligent Transport Systems (ITS); Testing; Conformance test specifications for Cooperative Awareness Basic Service (CA); Part 3: Abstract Test Suite (ATS) and Protocol Implementation eXtra Information for Testing (PIXIT)	published	Update according to changes in ETSI EN 302 627-2 and TS 103 097	

	Standardization Body	Title	Status	Summary	CitySCAPE Action
222.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 102 869-1 V1.6.1 (2020-04) Intelligent Transport Systems (ITS); Testing; Conformance test specifications for Decentralized Environmental Notification Basic Service (DEN); Part 1: Test requirements and Protocol Implementation Conformance Statement (PICS) pro forma	published	Update according to changes in ETSI EN 302 637-3 and TS 103 097	
223.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 102 869-2 V1.6.1 (2020-04) Intelligent Transport Systems (ITS); Testing; Conformance test specifications for Decentralized Environmental Notification Basic Service (DEN); Part 2: Test Suite Structure and Test Purposes (TSS & TP)	published	Update according to changes in ETSI EN 302 637-3 and TS 103 097	
224.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 102 869-3 V1.6.1 (2020-04) Intelligent Transport Systems (ITS); Testing; Conformance test specifications for Decentralized Environmental Notification Basic Service (DEN); Part 3: Abstract Test Suite (ATS) and Protocol Implementation eXtra Information for Testing (PIXIT)	published	Update according to changes in ETSI EN 302 637-2 and TS 103 097	
225.	ETSI TC ITS Intelligent Transport Systems	ETSI TR 101 607 V1.2.1 (2020-02) Intelligent Transport Systems (ITS); Cooperative ITS (C-ITS); Release 1	published	To update the ETSI deliverables that form Release 1 for Cooperative ITS.	

	Standardization Body	Title	Status	Summary	CitySCAPE Action
226.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 103 301 V1.3.1 (2020-02) Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Facilities layer protocols and communication requirements for infrastructure services	published	Revision of the TS 103 301 in order to extend the SSP of the current communication profiles and to add additional communication profiles for communications using IP technologies.	
227.	ETSI TC ITS Intelligent Transport Systems	ETSI TR 103 576-2 V1.1.1 (2020-02) Intelligent Transport Systems (ITS); Pre-standardization study on ITS architecture; Part 2: Interoperability among heterogeneous ITS systems and backward compatibility	published	The study item intends to investigate how to obtain Interoperability and backward compatibility when implementing future ITS architectures with the existing ETSI ITS specifications. This study item will elaborate the definitions of interoperability and backward compatibility	
228.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 102 965 V1.5.1 (2020-01) Intelligent Transport Systems (ITS); Application Object Identifier (ITS-AID); Registration	published	Extend the normative annex of document ETSI TS 102 965 v1.4.1 with new ITS-AIDs assigned for ETSI ITS by ISO. Particularly, the ITS-AIDs for the Collective Perception Service (ETSI TS 103 324), the Vulnerable Road Uses Awareness (ETSI TS 103 300), the TLC Request Service and the TLS Status Service (both ETSI TS 103 301). New AIDs have been assigned by ISO	
229.	ETSI TC ITS Intelligent Transport Systems	Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 4: Geographical addressing and forwarding for point-to-point and point-to-multipoint communications; Sub-part 1: Media-Independent Functionality	published	Incorporate revisions to support LTE-V2X in addition to ITS-G5. Revisions must be backward compatible for ITS-G5.	

	Standardization Body	Title	Status	Summary	CitySCAPE Action
230.	ETSI TC ITS Intelligent Transport Systems	ETSI EN 303 613 V1.1.1 (2020-01) Intelligent Transport Systems (ITS); LTE-V2X Access layer specification for Intelligent Transport Systems operating in the 5 GHz frequency band	published	To specify the access layer for the LTE-V2X technology	
231.	ETSI TC ITS Intelligent Transport Systems	ETSI EN 302 663 V1.3.1 (2020-01) Intelligent Transport Systems (ITS); ITS-G5 Access layer specification for Intelligent Transport Systems operating in the 5 GHz frequency band	published	Revision on the standard in order to address the following: - title update -clarifications and references updates -spotted errors	
232.	ETSI TC ITS Intelligent Transport Systems	ETSI TR 103 562 V2.1.1 (2019-12) Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Analysis of the Collective Perception Service (CPS); Release 2	published	The deliverable intends to clarify the technical concepts related to the exchange of sensor information between ITS-Ss and will be used as a baseline for the specification of CPS in ETSI TS 103 324	
233.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 103 152 V2.1.1 (2019-11) Intelligent Transport Systems (ITS); V2X Communications; Multimedia Content Dissemination (MCD) Basic Service specification; Release 2	published	Develop the Multimedia Content Dissemination basic service specification enabling the V2X exchange of multimedia information comprising video, audio, images and data. Messages can be exchanged through broadcast / multicast/unicast or peer to peer communication.	
234.	ETSI TC ITS Intelligent Transport Systems	ETSI TR 103 573 V1.1.1 (2019-11) Intelligent Transport Systems (ITS); Pre-standardization study of ITS test mode for operational devices in the field	published	The deliverable intends to define the way devices (DUTs) should be tested in the field assuming ITS-G5 as protocol of communication	

	Standardization Body	Title	Status	Summary	CitySCAPE Action
235.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 103 544-1 V1.3.1 (2019-10) Publicly Available Specification (PAS); Intelligent Transport Systems (ITS); Part 1: Connectivity	published	Definition of the lower layer wired and wireless connectivity protocols for MirrorLink. Integration of change requests based on feedback from plugfests and initial implementations undergoing CCC's MirrorLink device certification program.	
236.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 103 544-2 V1.3.1 (2019-10) Publicly Available Specification (PAS); Intelligent Transport Systems (ITS); Part 2: Virtual Network Computing (VNC) based Display and Control	published	Definition of the remote framebuffer streaming and user input back channel for MirrorLink using VNC. Integration of change requests based on feedback from plugfests and initial implementations undergoing CCC's MirrorLink device certification program.	
237.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 103 544-3 V1.3.1 (2019-10) Publicly Available Specification (PAS); Intelligent Transport Systems (ITS); Part 3: Audio	published	Definition of MirrorLink Audio, based on an RTP forward and back channel, plus an possible Bluetooth HFP and A2DP setup. Integration of change requests based on feedback from plugfests and initial implementations undergoing CCC's MirrorLink device certification program.	
238.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 103 544-4 V1.3.1 (2019-10) Publicly Available Specification (PAS); Intelligent Transport Systems (ITS); Part 4: Device Attestation Protocol (DAP)	published	Definition of device attestation protocol, creating the basic trust relationship between a MirrorLink Server and Client. Integration of change requests based on feedback from plugfests and initial implementations undergoing CCC's MirrorLink device certification program.	
239.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 103 544-5 V1.3.1 (2019-10) Publicly Available Specification (PAS); Intelligent Transport Systems (ITS); Part 5: Common Data Bus (CDB)	published	Definition of MirrorLink data exchange mechanism, allowing the launch, termination of individual data services at the MirrorLink Client and Server, and the transfer of individual data payload packets. Integration of change requests based on feedback from plugfests and initial implementations undergoing CCC's MirrorLink device certification program.	
240.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 103 544-6 V1.3.1 (2019-10) Publicly Available Specification (PAS); Intelligent Transport Systems (ITS); Part 6: Service Binary Protocol (SBP)	published	Definition of read, write and subscribe access to data objects of a MirrorLink data service. Binary protocol, carried within CDB data payload messages. Integration of change requests based on feedback from plugfests and initial implementations undergoing CCC's MirrorLink device certification program.	

	Standardization Body	Title	Status	Summary	CitySCAPE Action
241.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 103 544-7 V1.3.1 (2019-10) Publicly Available Specification (PAS); Intelligent Transport Systems (ITS); Part 7: GPS Data Service	published	Definition of a GPS Data Service, based on MirrorLink's CDB/SBP data exchange mechanism. Integration of change requests based on feedback from plugfests and initial implementations undergoing CCC's MirrorLink device certification program.	
242.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 103 544-8 V1.3.1 (2019-10) Publicly Available Specification (PAS); Intelligent Transport Systems (ITS); Part 8: Location Data Service	published	Definition of a high-level Location Data Service, based on MirrorLink's CDB/SBP data exchange mechanism. Integration of change requests based on feedback from plugfests and initial implementations undergoing CCC's MirrorLink device certification program.	
243.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 103 544-9 V1.3.1 (2019-10) Publicly Available Specification (PAS); Intelligent Transport Systems (ITS); Part 9: UPnP Application Server Service	published	Definition of a UPnP Service, allowing the UPnP Control Point to retrieve available MirrorLink applications, retrieve their certification related information and control them (launch, termination). Integration of change requests based on feedback from plugfests and initial implementations undergoing CCC's MirrorLink device certification program.	
244.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 103 544-10 V1.3.1 (2019-10) Publicly Available Specification (PAS); Intelligent Transport Systems (ITS); Part 10: UPnP Client Profile Service	published	Definition of a UPnP Service, allowing the UPnP Control Point to upload the MirrorLink Client's profile information, like manufacturer name etc. to the MirrorLink Server. Integration of change requests based on feedback from plugfests and initial implementations undergoing CCC's MirrorLink device certification program.	
245.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 103 544-11 V1.3.1 (2019-10) Publicly Available Specification (PAS); Intelligent Transport Systems (ITS); Part 11: UPnP Notification Server Service	published	Definition of a UPnP Service, allowing the UPnP Control Point to retrieve notifications from the UPnP Server and responding to them. Integration of change requests based on feedback from plugfests and initial implementations undergoing CCC's MirrorLink device certification program.	
246.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 103 544-12 V1.3.1 (2019-10) Publicly Available Specification (PAS); Intelligent Transport Systems (ITS); Part 12: UPnP Server Device	published	Definition of a UPnP Server, providing MirrorLink Services. Integration of change requests based on feedback from plugfests and initial implementations undergoing CCC's MirrorLink device certification program.	

	Standardization Body	Title	Status	Summary	CitySCAPE Action
247.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 103 544-13 V1.3.1 (2019-10) Publicly Available Specification (PAS); Intelligent Transport Systems (ITS); Part 13: Core Architecture	published	Definition of the MirrorLink Core architecture, linking the different MirrorLink related protocols together, and providing MirrorLink session related information. Integration of change requests based on feedback from plugfests and initial implementations undergoing CCC's MirrorLink device certification program.	
248.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 103 544-14 V1.3.1 (2019-10) Publicly Available Specification (PAS); Intelligent Transport Systems (ITS); Part 14: Application Certificates	published	Definition of the MirrorLink application certificates, and how MirrorLink Servers retrieve them from the central application certificate management system, check for revocation of them and present certificate related information to the MirrorLink Clients. Integration of change requests based on feedback from plugfests and initial implementations undergoing CCC's MirrorLink device certification program.	
249.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 103 544-15 V1.3.1 (2019-10) Publicly Available Specification (PAS); Intelligent Transport Systems (ITS); Part 15: Application Programming Interface (API) Level 1 & 2	published	Definition of the MirrorLink application programming interface, giving read/write access to underlying MirrorLink information. Integration of change requests based on feedback from plugfests and initial implementations undergoing CCC's MirrorLink device certification program.	
250.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 103 544-16 V1.3.1 (2019-10) Publicly Available Specification (PAS); Intelligent Transport Systems (ITS); Part 16: Application Developer Certificates	published	Definition of the MirrorLink application developer certificates, and how MirrorLink Servers retrieve them from the central application certificate management system, and check for revocation of them. Additionally, the document specifies how non-certified applications are presented as drive-certified application to the MirrorLink Client in a development mode. Integration of change requests based on feedback from plugfests and initial implementations undergoing CCC's MirrorLink device certification program.	
251.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 103 544-17 V1.3.1 (2019-10) Publicly Available Specification (PAS); Intelligent Transport Systems (ITS); Part 17: over Wi-Fi Display (WFD)	published	Definition of the remote framebuffer streaming and user input back channel for MirrorLink using Wi-Fi Display (WFD), including forward audio. Integration of change requests based on feedback from plugfests and initial implementations undergoing CCC's MirrorLink device certification program.	

	Standardization Body	Title	Status	Summary	CitySCAPE Action
252.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 103 544-18 V1.3.1 (2019-10) Publicly Available Specification (PAS); Intelligent Transport Systems (ITS); Part 18: IEEE 802.11TM Car Connectivity Consortium (CCC) Information Element	published	Definition of the IEEE 802.11 CCC Information Element, used to advertise availability of MirrorLink support. Integration of change requests based on feedback from plugfests and initial implementations undergoing CCC's MirrorLink device certification program.	
253.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 103 544-19 V1.3.1 (2019-10) Publicly Available Specification (PAS); Intelligent Transport Systems (ITS); Part 19: Network Information Data Service	published	Definition of a data service, which provides MirrorLink Server's network capabilities and status of the Wi-Fi Access Point to the MirrorLink Client. The data service is based on MirrorLink's CDB/SBP data exchange mechanism. Integration of change requests based on feedback from plugfests and initial implementations undergoing CCC's MirrorLink device certification program.	
254.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 103 544-20 V1.3.1 (2019-10) Publicly Available Specification (PAS); Intelligent Transport Systems (ITS); Part 20: Internet Accessibility	published	This document specifies MirrorLink Device Discovery on Wi-Fi Direct. The procedure is used to provide MirrorLink Server and Client's Internet configuration prior to Wi-Fi P2P group formation. Integration of change requests based on feedback from plugfests and initial implementations undergoing CCC's MirrorLink device certification program.	
255.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 103 544-21 V1.3.1 (2019-10) Publicly Available Specification (PAS); Intelligent Transport Systems (ITS); Part 21: High Speed Media Link (HSML)	published	Definition of remote framebuffer streaming over raw USB, using a vendor specific device class. Integration of change requests based on feedback from plugfests and initial implementations undergoing CCC's MirrorLink device certification program.	
256.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 103 544-22 V1.3.1 (2019-10) Publicly Available Specification (PAS); Intelligent Transport Systems (ITS); Part 22: Android Specific Specifications enabling AIDL-based Applications	published	Definition of Android specific MirrorLink behavior. The documents include required implementation details for MirrorLink Server devices, based on Android. Integration of change requests based on feedback from plugfests and initial implementations undergoing CCC's MirrorLink device certification program.	

	Standardization Body	Title	Status	Summary	CitySCAPE Action
257.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 103 544-23 V1.3.1 (2019-10) Publicly Available Specification (PAS); Intelligent Transport Systems (ITS); Part 23: Out-of-Band Pairing Data Service	published	Definition of a Bluetooth out-of-band Data Service, based on MirrorLink's CDB/SBP data exchange mechanism. Data service enables initial Bluetooth pairing, using the CDB/SBP infrastructure. Mechanism similar to Bluetooth out of band pairing using NFC. Integration of change requests based on feedback from plugfests and initial implementations undergoing CCC's MirrorLink device certification program.	
258.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 103 544-24 V1.3.1 (2019-10) Publicly Available Specification (PAS); Intelligent Transport Systems (ITS); Part 24: Media Meta Data Service	published	Definition of a Media Meta Data Service, based on MirrorLink's CDB/SBP data exchange mechanism. Integration of change requests based on feedback from plugfests and initial implementations undergoing CCC's MirrorLink device certification program.	
259.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 103 544-25 V1.3.1 (2019-10) Publicly Available Specification (PAS); Intelligent Transport Systems (ITS); Part 25: Navigation Meta Data Service	published	Definition of a Navigation Meta Data Service, based on MirrorLink's CDB/SBP data exchange mechanism. Integration of change requests based on feedback from plugfests and initial implementations undergoing CCC's MirrorLink device certification program.	
260.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 103 544-26 V1.3.1 (2019-10) Publicly Available Specification (PAS); Intelligent Transport Systems (ITS); Part 26: Consumer Experience Principles and Basic Features	published	Definition of MirrorLink specific consumer experience principles and respective MirrorLink features. The consumer experience requirements drive many other technical requirements. Integration of change requests based on feedback from plugfests and initial implementations undergoing CCC's MirrorLink device certification program.	
261.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 103 544-27 V1.3.1 (2019-10) Publicly Available Specification (PAS); Intelligent Transport Systems (ITS); Part 27: Basic Meta Data Service	published	Definition of a Basic Meta Data Service, based on MirrorLink's CDB/SBP data exchange mechanism. Serves as the parent class of other meta data services. Integration of change requests based on feedback from plugfests and initial implementations undergoing CCC's MirrorLink device certification program.	

	Standardization Body	Title	Status	Summary	CitySCAPE Action
262.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 103 544-28 V1.3.1 (2019-10) Publicly Available Specification (PAS); Intelligent Transport Systems (ITS); Part 28: Weather Data Service	published	Definition of a Weather Data Service, based on MirrorLink's CDB/SBP data exchange mechanism. Integration of change requests based on feedback from plugfests and initial implementations undergoing CCC's MirrorLink device certification program.	
263.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 103 544-29 V1.3.1 (2019-10) Publicly Available Specification (PAS); Intelligent Transport Systems (ITS); Part 29: Schedule Data Service	published	Definition of a Schedule Data Service, based on MirrorLink's CDB/SBP data exchange mechanism. Integration of change requests based on feedback from plugfests and initial implementations undergoing CCC's MirrorLink device certification program.	
264.	ETSI TC ITS Intelligent Transport Systems	ETSI TR 103 300-1 V2.1.1 (2019-09) Intelligent Transport System (ITS); Vulnerable Road Users (VRU) awareness; Part 1: Use Cases definition; Release 2	published	Definition of the VRU system and use cases (stage 1)	
265.	ETSI TC ITS Intelligent Transport Systems	ETSI EN 302 890-1 V1.2.1 (2019-07) Intelligent Transport Systems (ITS); Facilities layer function; Part 1: Services Announcement (SA) specification	published	European Norm of the services announcement technical specification (TS 102 890-1), which is part of the facilities layer' services management function	
266.	ETSI TC ITS Intelligent Transport Systems	ETSI TR 103 299 V2.1.1 (2019-06) Intelligent Transport System (ITS); Cooperative Adaptive Cruise Control (CACC); Pre-standardization study	published	To describe the relevant C-ACC use cases enabled by Cooperative ITS, considering the current state-of-the-art. To review the existing ITS standards in light of the described use cases. To identify and describe features at the ITS application and/or facilities layer to support the use cases. To make recommendations for further specifications for existing standards revision or new standard development.	
267.	ETSI TC ITS Intelligent Transport Systems	ETSI TR 103 257-1 V1.1.1 (2019-05) Intelligent Transport Systems (ITS); Access Layer; Part 1: Channel Models for the 5,9 GHz frequency band	published	The deliverable will provide a set of channel models describing how radio signals in the 5.9 GHz frequency band are perturbed by the mobile radio environment in several use cases.	

	Standardization Body	Title	Status	Summary	CitySCAPE Action
268.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 103 600 V1.1.1 (2019-05) Intelligent Transport Systems (ITS); Testing; Interoperability test specifications for security	published	To develop interoperability test descriptions to cover TS 103 097 v1.3.1, TS 102 941 v1.2.1, TS 102 940 v1.3.1	
269.	ETSI TC ITS Intelligent Transport Systems	ETSI EN 302 636-5-1 V2.2.1 (2019-05) Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 5: Transport Protocols; Sub-part 1: Basic Transport Protocol	published	Incorporate revisions to support LTE-V2X in addition to ITS-G5. Revisions must be backward compatible for ITS-G5.	
270.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 103 248 V1.3.1 (2019-04) Intelligent Transport Systems (ITS); GeoNetworking; Port Numbers for the Basic Transport Protocol (BTP)	published	Assign new BTP port numbers for newly defined services at Facilities layer (multimedia content dissemination service and Collective Perception service)	
271.	ETSI TC ITS Intelligent Transport Systems	ETSI EN 302 637-2 V1.4.1 (2019-04) Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service	published	Extending the Cooperative Awareness basic service to support the LTE-V2X access layer and communication profile. ITS-G5 backwards compatibility will be retained. To realize correct referencing to the right version of the CDD ETSI TS 102 894-2 V1.3.1.	
272.	ETSI TC ITS Intelligent Transport Systems	ETSI EN 302 637-3 V1.3.1 (2019-04) Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 3: Specifications of Decentralized Environmental Notification Basic Service	published	To realize correct referencing to the right version of the CDD ETSI TS 102 894-2 V1.3.1. Extending the specification of the "Decentralized Environmental Notification" basic service to support the LTE-V2X access layer and communication profile. Backwards compatibility for ITS-G5 will be preserved.	

	Standardization Body	Title	Status	Summary	CitySCAPE Action
273.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 103 525-1 V1.1.1 (2019-03) Intelligent Transport Systems (ITS); Testing; Conformance test specifications for ITS PKI management; Part 1: Protocol Implementation Conformance Statement (PICS)	published	To create PICS for PKI management based on ETSI TS 102 941	
274.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 103 525-2 V1.1.1 (2019-03) Intelligent Transport Systems (ITS); Testing; Conformance test specifications for ITS PKI management; Part 2: Test Suite Structure and Test Purposes (TSS & TP)	published	To create TSS&TP for PKI management based on ETSI TS 102 941	
275.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 103 525-3 V1.1.1 (2019-03) Intelligent Transport Systems (ITS); Testing; Conformance test specifications for ITS PKI management; Part 3: Abstract Test Suite (ATS) and Protocol Implementation eXtra Information for Testing (PIXIT)	published	To create ATS for PKI management based on ETSI TS 102 941	
276.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 102 941 V1.3.1 (2019-02) Intelligent Transport Systems (ITS); Security; Trust and Privacy Management	published	To update TS 102 941 V1.2.1 specification with corrections and clarifications provided for the ETSI ITS CMS6 Security plugtest	

	Standardization Body	Title	Status	Summary	CitySCAPE Action
277.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 102 636-7-1 V1.1.1 (2019-01) Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 7: Amendments for LTE-V2X; Sub-part 1: Amendments to ETSI EN 302 636-4-1 (Media-Independent Functionality)	published	The purpose of this deliverable is to amend EN 303 636-4-1 (Geonetworking Media-Independent Functionality) V1.3.1 in order to describe how to consider LTE-V2X technology	
278.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 102 636-7-2 V1.1.1 (2019-01) Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 7: Amendments for LTE-V2X; Sub-part 2: Amendments to ETSI EN 302 636-5-1 (Basic Transport Protocol)	published	The purpose of this deliverable is to amend EN 302 636-5-1 (Geonetworking Basic Transport Protocol) v2.1.1 in order to describe how to consider LTE-V2X technology.	
279.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 103 574 V1.1.1 (2018-11) Intelligent Transport Systems (ITS); Congestion Control Mechanisms for C-V2X PC5 interface; Access layer part	published	Specify intrasystem congestion control for the Cellular-V2X PC5 interface access layer including interfaces to other layers. Functionally similar to TS 102 687 for ITS-G5. The specification intends to address operation in bands intended for ITS, e.g. 5.9GHz.	
280.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 102 965 V1.4.1 (2018-11) Intelligent Transport Systems (ITS); Application Object Identifier (ITS-AID); Registration	published	Update registration list for SA.	
281.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 103 613 V1.1.1 (2018-11) Intelligent Transport Systems (ITS); Access layer specification for Intelligent Transport Systems using LTE Vehicle to everything communication in the 5,9 GHz frequency band	published	To define the physical layer and the data link layer and radio resource configuration, grouped into the access layer of the ITS station reference architecture EN 302 665. The access layer technology that is specified in the present document refers to what is known as the sidelink or PC5 interface of LTE Vehicle to everything (LTE-V2X) for the following frequency bands: <ul style="list-style-type: none"> - Operation in frequency band dedicated to ITS for safety related applications in the frequency range 5,875 GHz to 5,925 GHz. - Operation in frequency bands dedicated to ITS non-safety applications in the frequency range 5,855 GHz to 5,875 GHz. The LTE-V2X technology is based on 3GPP specifications.	

	Standardization Body	Title	Status	Summary	CitySCAPE Action
282.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 103 192-1 V1.1.1 (2018-09) Intelligent Transport Systems (ITS); Testing; Interoperability test specifications for ITS V2X use cases; Part 1: Test requirements and Interoperability Feature Statement (IFS) pro forma	published	Extraction of testable requirements and IFS from ITS V2X Use Cases	
283.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 103 192-2 V1.1.1 (2018-09) Intelligent Transport Systems (ITS); Testing; Interoperability test specifications for ITS V2X use cases; Part 2: Test Suite Structure and Test Purposes (TSS & TP)	published	Test Suite Structure and Test Purposes (TSS&TP) for the interoperability test scenarios	
284.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 103 192-3 V1.1.1 (2018-09) Intelligent Transport Systems (ITS); Testing; Interoperability test specifications for ITS V2X use cases; Part 3: Abstract Test Suite (ATS) and Protocol Implementation eXtra Information for Testing (PIXIT)	published	Tests in TTCN-3	
285.	ETSI TC ITS Intelligent Transport Systems	ETSI TR 103 193 V1.1.1 (2018-09) Intelligent Transport Systems (ITS); Testing; Interoperability test specifications for ITS V2X use cases; Architecture of ITS Interoperability Validation Framework	published	Description and documentation of the software packages	

	Standardization Body	Title	Status	Summary	CitySCAPE Action
286.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 102 708-2-2 V1.5.1 (2018-08) Intelligent Transport Systems (ITS); RTTT; Test specifications for High Data Rate (HDR) data transmission equipment operating in the 5,8 GHz ISM band; Part 2: Application Layer; Sub-Part 2: Test Suite Structure and Test Purposes (TSS & TP)	published	Revise and correct following points of the standard in order to cope with results from field implementation: Change test purpose TP/OBU/AL/SC/BV/07 to be applicable only for OBEs conforming to Security Level 0. Add a further test purpose for OBEs supporting Security Level 1. Check the document for other possible inconsistencies/errors of the same kind. Perform editorial changes and other minor technical changes when necessary.	
287.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 102 708-2-3 V1.5.1 (2018-08) Intelligent Transport Systems (ITS); RTTT; Test specifications for High Data Rate (HDR) data transmission equipment operating in the 5,8 GHz ISM band; Part 2: Application Layer; Sub-part 3: Abstract Test Suite (ATS) and partial PIXIT pro forma	published	Revise and correct following points of the standard in order to cope with results from field implementation: Change test purpose TP/OBU/AL/SC/BV/07 to be applicable only for OBEs conforming to Security Level 0. Add a further test purpose for OBEs supporting Security Level 1. Check the document for other possible inconsistencies/errors of the same kind. Perform editorial changes and other minor technical changes when necessary.	
288.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 103 096-1 V1.4.1 (2018-08) Intelligent Transport Systems (ITS); Testing; Conformance test specifications for ITS Security; Part 1: Protocol Implementation Conformance Statement (PICS)	published	To update PICS according to changes made in the last version of ETSI TS 103 097.	
289.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 103 096-2 V1.4.1 (2018-08) Intelligent Transport Systems (ITS); Testing; Conformance test specifications for ITS Security; Part 2: Test Suite Structure and Test Purposes (TSS & TP)	published	To update TSS&TP according to significant changes in TS 103 097.	

	Standardization Body	Title	Status	Summary	CitySCAPE Action
290.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 103 096-3 V1.4.1 (2018-08) Intelligent Transport Systems (ITS); Testing; Conformance test specifications for ITS Security; Part 3: Abstract Test Suite (ATS) and Protocol Implementation eXtra Information for Testing (PIXIT)	published	Develop a test suite for new tests of receiving and exceptional behaviour of ITS stations based on TS 103 097.	
291.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 103 248 V1.2.1 (2018-08) Intelligent Transport Systems (ITS); GeoNetworking; Port Numbers for the Basic Transport Protocol (BTP)	published	- Update references for existing port numbers - add new port numbers and their corresponding reference (service announcement)	
292.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 103 301 V1.2.1 (2018-08) Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Facilities layer protocols and communication requirements for infrastructure services	published	Update in order to revise existing communication profiles and to include additional ones based on 3GPP specifications.	
293.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 102 894-2 V1.3.1 (2018-08) Intelligent Transport Systems (ITS); Users and applications requirements; Part 2: Applications and facilities layer common data dictionary	published	Definition and specifications on the common data container at the applications and facilities layer. Revision of TS 102 894 - 2 V1.2.1 for bug fixing only.	
294.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 101 539-2 V1.1.1 (2018-06) Intelligent Transport Systems (ITS); V2X Applications; Part 2: Intersection Collision Risk Warning (ICRW) application requirements specification	published	Description of the Intersection Collision Risk Warning application and development of related specifications on the necessary parameters and conditions to operate the application using Co-operative Awareness Message (CAM) and / or of Decentralized Environmental Notification Message (DENM)	

	Standardization Body	Title	Status	Summary	CitySCAPE Action
295.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 102 941 V1.2.1 (2018-05) Intelligent Transport Systems (ITS); Security; Trust and Privacy Management	published	To update TS 102 941 to include specification for identity and key management functions, e.g. for issuing and managing long-term and short-term identities. To address updates in data structures identified in TS 103 097 and latest versions of IEEE 1609.2	
296.	ETSI TC ITS Intelligent Transport Systems	ETSI TR 103 415 V1.1.1 (2018-04) Intelligent Transport Systems (ITS); Security; Pre-standardization study on pseudonym change management	published	To realize an overview of the relevant pseudonym change strategies and solutions suitable for C-ITS (pseudonymous authentication based on PKI). To provide a comparison of the efficiency and the estimated performances of different pseudonym change strategies and identify relevant strategies to support various ITS-S profiles. The change rate of ITS-S credentials is a crucial parameter for protection of privacy. However, these strategies may have different impacts on the level of privacy, on communication overhead, storage and computation, as well as on costs. As pseudonym ID changes must be consistent across layers, pseudonym changes also have impact on C-ITS protocol stack performances (i.e. all stack layers has to change their IDs). To make recommendations for further specifications for existing standards revision or new standard development.	
297.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 102 687 V1.2.1 (2018-04) Intelligent Transport Systems (ITS); Decentralized Congestion Control Mechanisms for Intelligent Transport Systems operating in the 5 GHz range; Access layer part	published	Streamline this TS with the set of DCC deliverables specified for other layers, e.g. DCC profile specifications; improvement of specific DCC requirements.	
298.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 102 940 V1.3.1 (2018-04) Intelligent Transport Systems (ITS); Security; ITS communications security architecture and security management	published	To revise the security architecture to add the role of the Trust List Manager, to revise services and to make minor corrections	
299.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 103 097 V1.3.1 (2017-10) Intelligent Transport Systems (ITS); Security; Security header and certificate formats	published	To extend TS 103 097 to support new EC crypto curves and provide adaptations to support crypto-agility, certificates profiles for new authorities (e.g. issuers of CTL/TSL, of CRL, ...).	

	Standardization Body	Title	Status	Summary	CitySCAPE Action
300.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 103 544-1 V1.3.0 (2017-10) Publicly Available Specification (PAS); Intelligent Transport Systems (ITS); Part 1: Connectivity	published	Definition of the lower layer wired and wireless connectivity protocols for MirrorLink	
301.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 103 544-2 V1.3.0 (2017-10) Publicly Available Specification (PAS); Intelligent Transport Systems (ITS); Part 2: Virtual Network Computing (VNC) based Display and Control	published	Definition of the remote framebuffer streaming and user input back channel for MirrorLink using VNC	
302.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 103 544-3 V1.3.0 (2017-10) Publicly Available Specification (PAS); Intelligent Transport Systems (ITS); Part 3: Audio	published	Definition of MirrorLink Audio, based on an RTP forward and back channel, plus an possible Bluetooth HFP and A2DP setup.	
303.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 103 544-4 V1.3.0 (2017-10) Publicly Available Specification (PAS); Intelligent Transport Systems (ITS); Part 4: Device Attestation Protocol (DAP)	published	Definition of device attestation protocol, creating the basic trust relationship between a MirrorLink Server and Client.	
304.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 103 544-5 V1.3.0 (2017-10) Publicly Available Specification (PAS); Intelligent Transport Systems (ITS); Part 5: Common Data Bus (CDB)	published	Definition of MirrorLink data exchange mechanism, allowing the launch, termination of individual data services at the MirrorLink Client and Server, and the transfer of individual data payload packets.	
305.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 103 544-6 V1.3.0 (2017-10) Publicly Available Specification (PAS); Intelligent Transport Systems (ITS); Part 6: Service Binary Protocol (SBP)	published	Definition of read, write and subscribe access to data objects of a MirrorLink data service. Binary protocol, carried within CDB data payload messages.	

	Standardization Body	Title	Status	Summary	CitySCAPE Action
306.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 103 544-7 V1.3.0 (2017-10) Publicly Available Specification (PAS); Intelligent Transport Systems (ITS); Part 7: GPS Data Service	published	Definition of a GPS Data Service, based on MirrorLink's CDB/SBP data exchange mechanism.	
307.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 103 544-8 V1.3.0 (2017-10) Publicly Available Specification (PAS); Intelligent Transport Systems (ITS); Part 8: Location Data Service	published	Definition of a high-level Location Data Service, based on MirrorLink's CDB/SBP data exchange mechanism.	
308.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 103 544-9 V1.3.0 (2017-10) Publicly Available Specification (PAS); Intelligent Transport Systems (ITS); Part 9: UPnP Application Server Service	published	Definition of a UPnP Service, allowing the UPnP Control Point to retrieve available MirrorLink applications, retrieve their certification related information and control them (launch, termination).	
309.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 103 544-10 V1.3.0 (2017-10) Publicly Available Specification (PAS); Intelligent Transport Systems (ITS); Part 10: UPnP Client Profile Service	published	Definition of a UPnP Service, allowing the UPnP Control Point to upload the MirrorLink Client's profile information, like manufacturer name etc. to the MirrorLink Server.	
310.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 103 544-11 V1.3.0 (2017-10) Publicly Available Specification (PAS); Intelligent Transport Systems (ITS); Part 11: UPnP Notification Server Service	published	Definition of a UPnP Service, allowing the UPnP Control Point to retrieve notifications from the UPnP Server and responding to them.	
311.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 103 544-12 V1.3.0 (2017-10) Publicly Available Specification (PAS); Intelligent Transport Systems (ITS); Part 12: UPnP Server Device	published	Definition of a UPnP Server, providing MirrorLink Services.	

	Standardization Body	Title	Status	Summary	CitySCAPE Action
312.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 103 544-13 V1.3.0 (2017-10) Publicly Available Specification (PAS); Intelligent Transport Systems (ITS); Part 13: Core Architecture	published	Definition of the MirrorLink Core architecture, linking the different MirrorLink related protocols together, and providing MirrorLink session related information.	
313.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 103 544-14 V1.3.0 (2017-10) Publicly Available Specification (PAS); Intelligent Transport Systems (ITS); Part 14: Application Certificates	published	Definition of the MirrorLink application certificates, and how MirrorLink Servers retrieve them from the central application certificate management system, check for revocation of them and present certificate related information to the MirrorLink Clients.	
314.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 103 544-15 V1.3.0 (2017-10) Publicly Available Specification (PAS); Intelligent Transport Systems (ITS); Part 15: Application Programming Interface (API) Level 1 & 2	published	Definition of the MirrorLink application programming interface, giving read/write access to underlying MirrorLink information.	
315.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 103 544-16 V1.3.0 (2017-10) Publicly Available Specification (PAS); Intelligent Transport Systems (ITS); Part 16: Application Developer Certificates	published	Definition of the MirrorLink application developer certificates, and how MirrorLink Servers retrieve them from the central application certificate management system and check for revocation of them. Additionally, the document specifies how non-certified applications are presented as drive-certified application to the MirrorLink Client in a development mode.	
316.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 103 544-17 V1.3.0 (2017-10) Publicly Available Specification (PAS); Intelligent Transport Systems (ITS); Part 17: over Wi-Fi Display (WFD)	published	Definition of the remote framebuffer streaming and user input back channel for MirrorLink using Wi-Fi Display (WFD), including forward audio.	

	Standardization Body	Title	Status	Summary	CitySCAPE Action
317.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 103 544-18 V1.3.0 (2017-10) Publicly Available Specification (PAS); Intelligent Transport Systems (ITS); Part 18: IEEE 802.11TM Car Connectivity Consortium (CCC) Information Element	published	Definition of the IEEE 802.11 CCC Information Element, used to advertise availability of MirrorLink support.	
318.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 103 544-19 V1.3.0 (2017-10) Publicly Available Specification (PAS); Intelligent Transport Systems (ITS); Part 19: Network Information Data Service	published	Definition of a data service, which provides MirrorLink Server's network capabilities and status of the Wi-Fi Access Point to the MirrorLink Client. The data service is based on MirrorLink's CDB/SBP data exchange mechanism.	
319.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 103 544-20 V1.3.0 (2017-10) Publicly Available Specification (PAS); Intelligent Transport Systems (ITS); Part 20: Internet Accessibility	published	This document specifies MirrorLink Device Discovery on Wi-Fi Direct. The procedure is used to provide MirrorLink Server and Client's Internet configuration prior to Wi-Fi P2P group formation.	
320.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 103 544-21 V1.3.0 (2017-10) Publicly Available Specification (PAS); Intelligent Transport Systems (ITS); Part 21: High Speed Media Link (HSML)	published	Definition of remote framebuffer streaming over raw USB, using a vendor specific device class.	
321.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 103 544-22 V1.3.0 (2017-10) Publicly Available Specification (PAS); Intelligent Transport Systems (ITS); Part 22: Android Specific Specifications enabling AIDL-based Applications	published	Definition of Android specific MirrorLink behaviour. The documents include required implementation details for MirrorLink Server devices, based on Android.	

	Standardization Body	Title	Status	Summary	CitySCAPE Action
322.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 103 544-23 V1.3.0 (2017-10) Publicly Available Specification (PAS); Intelligent Transport Systems (ITS); Part 23: Out-of-Band Pairing Data Service	published	Definition of a Bluetooth out-of-band Data Service, based on MirrorLink's CDB/SBP data exchange mechanism. Data service enables initial Bluetooth pairing, using the CDB/SBP infrastructure. Mechanism similar to Bluetooth out of band pairing using NFC.	
323.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 103 544-24 V1.3.0 (2017-10) Publicly Available Specification (PAS); Intelligent Transport Systems (ITS); Part 24: Media Meta Data Service	published	Definition of a Media Meta Data Service, based on MirrorLink's CDB/SBP data exchange mechanism.	
324.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 103 544-25 V1.3.0 (2017-10) Publicly Available Specification (PAS); Intelligent Transport Systems (ITS); Part 25: Navigation Meta Data Service	published	Definition of a Navigation Meta Data Service, based on MirrorLink's CDB/SBP data exchange mechanism.	
325.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 103 544-26 V1.3.0 (2017-10) Publicly Available Specification (PAS); Intelligent Transport Systems (ITS); Part 26: Consumer Experience Principles and Basic Features	published	Definition of MirrorLink specific consumer experience principles and respective MirrorLink features. The consumer experience requirements drive many other technical requirements.	
326.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 103 544-27 V1.3.0 (2017-10) Publicly Available Specification (PAS); Intelligent Transport Systems (ITS); Part 27: Basic Meta Data Service	published	Definition of a Basic Meta Data Service, based on MirrorLink's CDB/SBP data exchange mechanism. Serves as the parent class of other meta data services.	

	Standardization Body	Title	Status	Summary	CitySCAPE Action
327.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 103 544-28 V1.3.0 (2017-10) Publicly Available Specification (PAS); Intelligent Transport Systems (ITS); Part 28: Weather Data Service	published	Definition of a Weather Data Service, based on MirrorLink's CDB/SBP data exchange mechanism.	
328.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 103 544-29 V1.3.0 (2017-10) Publicly Available Specification (PAS); Intelligent Transport Systems (ITS); Part 29: Schedule Data Service	published	Definition of a Schedule Data Service, based on MirrorLink's CDB/SBP data exchange mechanism.	
329.	ETSI TC ITS Intelligent Transport Systems	ETSI EN 302 636-4-1 V1.3.1 (2017-08) Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 4: Geographical addressing and forwarding for point-to-point and point-to-multipoint communications; Sub-part 1: Media-Independent Functionality	published	Corrections of the GeoNetworking for media-independent operations, excluding the specification of new functions	
330.	ETSI TC ITS Intelligent Transport Systems	ETSI EN 302 636-5-1 V2.1.1 (2017-08) Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 5: Transport Protocols; Sub-part 1: Basic Transport Protocol	published	Revision of the EN 302 636 - 5 - 1, harmonization with DTS/ITS-00351 - TS 103 248 BTP Port numbers; definition of values for destination port info	

	Standardization Body	Title	Status	Summary	CitySCAPE Action
331.	ETSI TC ITS Intelligent Transport Systems	ETSI TR 103 403 V1.1.1 (2017-06) Intelligent Transport Systems (ITS); Mitigation techniques to avoid harmful interference between equipment compliant with ES 200 674-1 and ITS operating in the 5 GHz frequency range; Evaluation of mitigation methods and techniques	published	Report of test executions and results of tests performed with equipment compliant with ES 200 674-1 and equipment compliant with IEEE 802.11 operating in the 5 GHz frequency band.	
332.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 102 871-1 V1.4.1 (2017-05) Intelligent Transport Systems (ITS); Testing; Conformance test specifications for GeoNetworking ITS-G5; Part 1: Test requirements and Protocol Implementation Conformance Statement (PICS) pro forma	published	Update according to feedback from Validation and CDD changes.	
333.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 102 871-2 V1.4.1 (2017-05) Intelligent Transport Systems (ITS); Testing; Conformance test specifications for GeoNetworking ITS-G5; Part 2: Test Suite Structure and Test Purposes (TSS & TP)	published	Update according to feedback from Validation and CDD changes.	
334.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 102 871-3 V1.4.1 (2017-05) Intelligent Transport Systems (ITS); Testing; Conformance test specifications for GeoNetworking ITS-G5; Part 3: Abstract Test Suite (ATS) and Protocol Implementation eXtra Information for Testing (PIXIT)	published	Update according to feedback from Validation and CDD changes.	

	Standardization Body	Title	Status	Summary	CitySCAPE Action
335.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 102 890-1 V1.1.1 (2017-05) Intelligent Transport Systems (ITS); Facilities layer function; Part 1: Services Announcement (SA) specification	published	Development of the Technical Specification of the services announcement which is part of the facilities layer' services management function	
336.	ETSI TC ITS Intelligent Transport Systems	ETSI TR 102 893 V1.2.1 (2017-03) Intelligent Transport Systems (ITS); Security; Threat, Vulnerability and Risk Analysis (TVRA)	published	Update to address those threats arising from consideration of the network and transport protocols (e.g. GeoNet, IP). In addition, address any updates arising from update of the BSA.	
337.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 103 096-1 V1.3.1 (2017-03) Intelligent Transport Systems (ITS); Testing; Conformance test specifications for ITS Security; Part 1: Protocol Implementation Conformance Statement (PICS)	published	To add PICS items related to additional tests of receiving and exceptional behaviour of ITS stations based on TS 103 097.	
338.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 103 096-2 V1.3.1 (2017-03) Intelligent Transport Systems (ITS); Testing; Conformance test specifications for ITS Security; Part 2: Test Suite Structure and Test Purposes (TSS & TP)	published	To include tests of receiving and exceptional behaviour of ITS stations based on TS 103 097. The new tests shall be limited to the test groups SEC/ITS-S/ S-DATA and SEC/ITS-S/R-DATA. The delivered tests will all be optional tests,	
339.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 103 096-3 V1.3.1 (2017-03) Intelligent Transport Systems (ITS); Testing; Conformance test specifications for ITS Security; Part 3: Abstract Test Suite (ATS) and Protocol Implementation eXtra Information for Testing (PIXIT)	published	Develop a test suite for new tests of receiving and exceptional behaviour of ITS stations based on TS 103 097.	

	Standardization Body	Title	Status	Summary	CitySCAPE Action
340.	ETSI TC ITS Intelligent Transport Systems	ETSI TR 103 099 V1.4.1 (2017-03) Intelligent Transport Systems (ITS); Architecture of conformance validation framework	published	Update based on validation feedback and SPat/MAP TS 103 031 v1.1.1.	
341.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 102 869-1 V1.5.1 (2017-03) Intelligent Transport Systems (ITS); Testing; Conformance test specifications for Decentralized Environmental Notification Basic Service (DEN); Part 1: Test requirements and Protocol Implementation Conformance Statement (PICS) pro forma	published	Update according to feedback from Validation and CDD changes.	
342.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 102 869-2 V1.5.1 (2017-03) Intelligent Transport Systems (ITS); Testing; Conformance test specifications for Decentralized Environmental Notification Basic Service (DEN); Part 2: Test Suite Structure and Test Purposes (TSS & TP)	published	Update according to feedback from Validation and CDD changes.	
343.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 102 869-3 V1.5.1 (2017-03) Intelligent Transport Systems (ITS); Testing; Conformance test specifications for Decentralized Environmental Notification Basic Service (DEN); Part 2: Test Suite Structure and Test Purposes (TSS & TP)	published	Update according to feedback from Validation and CDD changes.	

	Standardization Body	Title	Status	Summary	CitySCAPE Action
344.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 103 191-1 V1.2.1 (2017-03) Intelligent Transport Systems (ITS); Testing; Conformance test specifications for Facilities layer protocols and communication requirements for infrastructure services; Part 1: Test requirements and Protocol Implementation Conformance Statement (PICS) pro forma	published	Update according to TS 103 301.	
345.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 103 191-2 V1.2.1 (2017-03) Intelligent Transport Systems (ITS); Testing; Conformance test specifications for Facilities layer protocols and communication requirements for infrastructure services; Part 2: Test Suite Structure and Test Purposes (TSS & TP)	published	Update to TS 103 301.	
346.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 103 191-3 V1.2.1 (2017-03) Intelligent Transport Systems (ITS); Testing; Conformance test specifications for Facilities layer protocols and communication requirements for infrastructure services; Part 3: Abstract Test Suite (ATS) and Protocol Implementation eXtra Information for Testing (PIXIT)	published	Update to TS 103 301.	

	Standardization Body	Title	Status	Summary	CitySCAPE Action
347.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 102 868-1 V1.4.1 (2017-03) Intelligent Transport Systems (ITS); Testing; Conformance test specifications for Cooperative Awareness Basic Service (CA); Part 1: Test requirements and Protocol Implementation Conformance Statement (PICS) pro forma	published	Update according to feedback from Validation and CDD changes	
348.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 102 868-2 V1.4.1 (2017-03) Intelligent Transport Systems (ITS); Testing; Conformance test specifications for Cooperative Awareness Basic Service (CA); Part 2: Test Suite Structure and Test Purposes (TSS & TP)	published	Update according to feedback from Validation and CDD changes.	
349.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 102 868-3 V1.4.1 (2017-03) Intelligent Transport Systems (ITS); Testing; Conformance test specifications for Cooperative Awareness Basic Service (CA); Part 3: Abstract Test Suite (ATS) and Protocol Implementation eXtra Information for Testing (PIXIT)	published	Update according to feedback from Validation and CDD changes.	
350.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 103 248 V1.1.1 (2016-11) Intelligent Transport Systems (ITS); GeoNetworking; Port Numbers for the Basic Transport Protocol (BTP)	published	The deliverable specifies and extends the port numbers for the Basic Transport Protocol as specified in EN 302 636-4-1. EN 302 636-4-1 v1.2.1 annex B serves as an initial input to the deliverable.	

	Standardization Body	Title	Status	Summary	CitySCAPE Action
351.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 102 965 V1.3.1 (2016-11) Intelligent Transport Systems (ITS); Application Object Identifier (ITS-AID); Registration	published	Update registration list by recently assigned ITS-AID values. Consider ISO 17419.	
352.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 103 301 V1.1.1 (2016-11) Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Facilities layer protocols and communication requirements for infrastructure services	published	The WI is to define specification at the facilities layer services to support communications from and/or to an infrastructure ITS-S (road side ITS-S or central ITS-S). It describes the related protocol handling for selected messages and specifies requirements to lower layer protocol stacks and to the security entity in order to support message dissemination and reception.	
353.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 102 940 V1.2.1 (2016-11) Intelligent Transport Systems (ITS); Security; ITS communications security architecture and security management	published	This WI addresses maintenance of TS 102 940 to address improvement on key management and IDs change in communication synchronized with pseudonym certificate change within the overall scope of ITS Release 1.	
354.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 102 723-8 V1.1.1 (2016-04) Intelligent Transport Systems (ITS); OSI cross-layer topics; Part 8: Interface between security entity and network and transport layer	published	Specifies Interface(s) between the ITS security entity and the ITS network&transport layer including interface services and service primitives which are extendible in order to achieve general applicability. Specifies related procedures and common parameters. Development is with consultation of TC ITS WG3 and WG2.	
355.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 101 556-2 V1.1.1 (2016-02) Intelligent Transport Systems (ITS); Infrastructure to Vehicle Communication; Part 2: Communication system specification to support application requirements for Tyre Information System (TIS) and Tyre Pressure Gauge (TPG) interoperability	published	Specification of the communication system required to support CEN functional and operational requirements for Tyre Pressure Monitoring System (TPMS). This includes system protocols to provide the communication between a road side Tyre Pressure Gauge (TPG) and the vehicle equipped with TPMS (Tyre Pressure Monitoring System).	

	Standardization Body	Title	Status	Summary	CitySCAPE Action
356.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 103 191-1 V1.1.1 (2015-09) Intelligent Transport Systems (ITS); Testing; Conformance test specifications for Signal Phase And Timing (SPAT) and Map (MAP); Part 1: Test requirements and Protocol Implementation Conformance Statement (PICS) pro forma	published	Development of the SPAT/MAP Implementation Conformance Statement (ICS) proforma	
357.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 103 191-2 V1.1.1 (2015-09) Intelligent Transport Systems (ITS); Testing; Conformance test specifications for Signal Phase And Timing (SPAT) and Map (MAP); Part 2: Test Suite Structure and Test Purposes (TSS & TP)	published	Development of SPAT/MAP Test Suite Structure and Test Purposes (TSS&TP).	
358.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 103 191-3 V1.1.1 (2015-09) Intelligent Transport Systems (ITS); Testing; Conformance test specifications for Signal Phase And Timing (SPAT) and Map (MAP); Part 3: Abstract Test Suite (ATS) and Protocol Implementation eXtra Information for Testing (PIXIT)	published	Development of the SPAT/MAP Abstract Test Suite (ATS) and Implementation eXtra Information for Testing (IXIT).	
359.	ETSI TC ITS Intelligent Transport Systems	ETSI TR 101 613 V1.1.1 (2015-09) Intelligent Transport Systems (ITS); Cross Layer DCC Management Entity for operation in the ITS G5A and ITS G5B medium; Validation set-up and results	published	This work item will cover the overall validation of the cross layer DCC functionality of the ETSI ITS architecture. It will consider the inputs from the cross layer DCC specification developed in DTS/ITS-0020046, the cross layer algorithm description in DTR/ITS-0020055. And the DCC specifications developed in the other relevant layers (DCC-Facility, DCC_Net, DCC_Access). This report is intended to support the test specification to be developed in a future WI.	

	Standardization Body	Title	Status	Summary	CitySCAPE Action
360.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 103 096-1 V1.2.1 (2015-09) Intelligent Transport Systems (ITS); Testing; Conformance test specifications for ITS Security; Part 1: Protocol Implementation Conformance Statement (PICS)	published	Update the PICS regarding ITS use of IEEE 1609.2 messages and data structures defined in TS 102 941 and TS 103 097.	
361.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 103 096-2 V1.2.1 (2015-09) Intelligent Transport Systems (ITS); Testing; Conformance test specifications for ITS Security; Part 2: Test Suite Structure and Test Purposes (TSS & TP)	published	Update the TSS&TP regarding ITS use of IEEE 1609.2 messages and data structures defined in TS 102 941 and TS 103 097.	
362.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 103 096-3 V1.2.1 (2015-09) Intelligent Transport Systems (ITS); Testing; Conformance test specifications for ITS Security; Part 3: Abstract Test Suite (ATS) and Protocol Implementation eXtra Information for Testing (PIXIT)	published	Develop a test suite for tests of ITS use of IEEE 1609.2 messages and data structures defined in TS 102 941 and TS 103 097.	
363.	ETSI TC ITS Intelligent Transport Systems	ETSI TR 103 061-6 V1.1.1 (2015-09) Intelligent Transport Systems (ITS); Testing; Conformance test specifications for ITS Security; Part 6: Validation report	published	Provides the validation report from the tests of ITS use of IEEE 1609.2 messages and data structures defined in TS 102 941 and TS 103 097.	

	Standardization Body	Title	Status	Summary	CitySCAPE Action
364.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 102 868-1 V1.3.1 (2015-07) Intelligent Transport Systems (ITS); Testing; Conformance test specifications for Cooperative Awareness Basic Service (CA); Part 1: Test requirements and Protocol Implementation Conformance Statement (PICS) pro forma	published	Update according to EN 302 637-2 (CAM) submitted to national vote	
365.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 102 868-2 V1.3.1 (2015-07) Intelligent Transport Systems (ITS); Testing; Conformance test specifications for Cooperative Awareness Basic Service (CA); Part 2: Test Suite Structure and Test Purposes (TSS & TP)	published	Update according to EN 302 637-2 (CAM) submitted to national vote	
366.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 102 868-3 V1.3.1 (2015-07) Intelligent Transport Systems (ITS); Testing; Conformance test specifications for Cooperative Awareness Basic Service (CA); Part 3: Abstract Test Suite (ATS) and Protocol Implementation eXtra Information for Testing (PIXIT)	published	Maintenance of the CAM Abstract Test Suite (ATS) and Protocol Implementation eXtra Information for Testing (PIXIT).	

	Standardization Body	Title	Status	Summary	CitySCAPE Action
367.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 102 869-1 V1.4.1 (2015-07) Intelligent Transport Systems (ITS); Testing; Conformance test specifications for Decentralized Environmental Notification Basic Service (DEN); Part 1: Test requirements and Protocol Implementation Conformance Statement (PICS) pro forma	published	Update according to EN 302 637-3 (DENM) submitted to national vote.	
368.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 102 869-2 V1.4.1 (2015-07) Intelligent Transport Systems (ITS); Testing; Conformance test specifications for Decentralized Environmental Notification Basic Service (DEN); Part 2: Test Suite Structure and Test Purposes (TSS & TP)	published	Update according to EN 302 637-3 (DENM) submitted to national vote.	
369.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 102 869-3 V1.4.1 (2015-07) Intelligent Transport Systems (ITS); Testing; Conformance test specifications for Decentralized Environmental Notification Basic Service (DEN); Part 3: Abstract Test Suite (ATS) and Protocol Implementation eXtra Information for Testing (PIXIT)	published	Update according to EN 302 637-3 (DENM) submitted to national vote.	
370.	ETSI TC ITS Intelligent Transport Systems	ETSI TR 103 099 V1.3.1 (2015-07) Intelligent Transport Systems (ITS); Architecture of conformance validation framework	published	Update of architecture design to allow for a common platform and a protocol-specific adaptations	

	Standardization Body	Title	Status	Summary	CitySCAPE Action
371.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 102 871-1 V1.3.1 (2015-06) Intelligent Transport Systems (ITS); Testing; Conformance test specifications for GeoNetworking ITS-G5; Part 1: Test requirements and Protocol Implementation Conformance Statement (PICS) pro forma	published	Update according to EN 302 636-4-1 (GN) submitted to national vote	
372.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 102 871-2 V1.3.1 (2015-06) Intelligent Transport Systems (ITS); Testing; Conformance test specifications for GeoNetworking ITS-G5; Part 2: Test Suite Structure and Test Purposes (TSS & TP)	published	Update according to EN 302 636-4-1 (GN) submitted to national vote	
373.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 102 871-3 V1.3.1 (2015-06) Intelligent Transport Systems (ITS); Testing; Conformance test specifications for GeoNetworking ITS-G5; Part 3: Abstract Test Suite (ATS) and Protocol Implementation eXtra Information for Testing (PIXIT)	published	Update according to EN 302 636-4-1 (GN) submitted to national vote	

	Standardization Body	Title	Status	Summary	CitySCAPE Action
374.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 102 792 V1.2.1 (2015-06) Intelligent Transport Systems (ITS); Mitigation techniques to avoid interference between European CEN Dedicated Short Range Communication (CEN DSRC) equipment and Intelligent Transport Systems (ITS) operating in the 5 GHz frequency range	published	Data elements to transmit the position(s) of CEN DSRC equipment have been included in EN 302 637-2 (CAM). The new version of TS 102 792 shall further detail the definition of its mitigation techniques by making use of these data elements. The work item also includes editorial changes to improve the standard.	
375.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 103 175 V1.1.1 (2015-06) Intelligent Transport Systems (ITS); Cross Layer DCC Management Entity for operation in the ITS G5A and ITS G5B medium	published	This work item will specify the functionality of the centralized DCC control entity including the required interfaces and parameters for controlling the DCC mechanisms in the facility layer, network and transport layer and the access layer. The centralized DCC entity will be responsible of evaluating the actual DCC state of the active ITS G5A and ITS G5B channels based on status information from the access layer, the network layer and the facility layer. In addition, the DCC status should be predicted for the following transmission intervals.	
376.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 103 097 V1.2.1 (2015-06) Intelligent Transport Systems (ITS); Security; Security header and certificate formats	published	To update V1.1.1 of the specification with corrections and clarifications arising from experience in implementation and plug-tests. The updates only address the TLS encoding model.	
377.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 102 965 V1.2.1 (2015-06) Intelligent Transport Systems (ITS); Application Object Identifier (ITS-AID); Registration	published	Upgrade TR to a TS Replace Annex B (snapshot of number assignments) by a hyperlink to the online info page at ISO Replace Annex A by a hyperlink to the template online at ISO Fix editorial and technical bugs.	
378.	ETSI TC ITS Intelligent Transport Systems	ETSI EN 302 636-3 V1.2.1 (2014-12) Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 3: Network Architecture	published	Revision of the TS 102 636 - 3 according to ETSI TC ITS work progress; harmonization as far as possible with other standardization work and received change requests before proposing it as an EN in conformity with M/453 mandate.	

	Standardization Body	Title	Status	Summary	CitySCAPE Action
379.	ETSI TC ITS Intelligent Transport Systems	ETSI EN 302 637-2 V1.3.2 (2014-11) Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service	published	Revision of the TS 102 637-2 according to ETSI TC ITS work progression and received Change Requests. Proposal to an EN in conformity to the M/453 mandate request.	
380.	ETSI TC ITS Intelligent Transport Systems	ETSI EN 302 637-3 V1.2.2 (2014-11) Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 3: Specifications of Decentralized Environmental Notification Basic Service	published	Revision of the TS 102 637 - 3 according to ETSI TC ITS work progression, harmonization as far as possible with other standardization work and received change requests before proposing it as an EN in conformity with M/453 mandate.	
381.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 101 556-3 V1.1.1 (2014-10) Intelligent Transport Systems (ITS); Infrastructure to Vehicle Communications; Part 3: Communications system for the planning and reservation of EV energy supply using wireless networks	published	The scope of this document is the specification of wireless application protocols and messages supporting the discovery of offered services (completing related discovery protocols), charging spot reservation (and possible renegotiation), pre-payment of the service reservation in the vehicle (involving pre-payment support or contract validation), and application-level logical pairing of the Electric Vehicle to a selected charging spot. Requirements regarding the underlying transport and network layer services will be also defined. This process starts from the journey planning phase and continues during the driving phase, terminating with the approach of the reserved parking / fast recharge / quick drop area. The work will be achieved in consistency with the ongoing standardisation, e.g. ISO/IEC 15118, IEC 62196-2. The scope includes support of different electrical energy provisioning modes, such as wired, quick drop or inductive recharging.	
382.	ETSI TC ITS Intelligent Transport Systems	ETSI EN 302 895 V1.1.1 (2014-09) Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Local Dynamic Map (LDM)	published	Scoping the Local Dynamic Map standardization and developing the related technical specification.	

	Standardization Body	Title	Status	Summary	CitySCAPE Action
383.	ETSI TC ITS Intelligent Transport Systems	ETSI TR 101 612 V1.1.1 (2014-09) Intelligent Transport Systems (ITS); Cross Layer DCC Management Entity for operation in the ITS G5A and ITS G5B medium; Report on Cross layer DCC algorithms and performance evaluation	published	This work item will provide a technical overview over the needed cross layer DCC algorithms to be implemented into the DCC management entity. The report will describe the algorithms in detail and will include performance evaluation results based on simulations. The report will include cross layer power control algorithms in support of the DCC functionality, a rate control algorithm and the needed parameter management functionalities. The report will be the bases for the specification of the cross layer DCC management entity in WI DTS/ITS-0020046 and the validation of the entity in DTR/ITS-0020056.	
384.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 102 894-2 V1.2.1 (2014-09) Intelligent Transport Systems (ITS); Users and applications requirements; Part 2: Applications and facilities layer common data dictionary	published	Revision of the common data container at the applications and facilities layer in order to meet current CAM and DENM requirements.	
385.	ETSI TC ITS Intelligent Transport Systems	ETSI EN 302 636-5-1 V1.2.1 (2014-08) Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 5: Transport Protocols; Sub-part 1: Basic Transport Protocol	published	Revision of the TS 102 636 - 5 - 1 according to ETSI TC ITS work progress; harmonization as far as possible with other standardization work and received change requests before proposing it as an EN in conformity with M/453 mandate.	
386.	ETSI TC ITS Intelligent Transport Systems	ETSI EN 302 636-4-1 V1.2.1 (2014-07) Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 4: Geographical addressing and forwarding for point-to-point and point-to-multipoint communications; Sub-part 1: Media-Independent Functionality	published	Revision of the TS 102 636 - 4 - 1 according to ETSI TC ITS work progress; harmonization as far as possible with other standardization work and received change requests before proposing it as an EN in conformity with M/453 mandate.	

	Standardization Body	Title	Status	Summary	CitySCAPE Action
387.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 102 760-1 V1.2.1 (2014-06) Intelligent Transport Systems (ITS); Communications Access for Land Mobiles (CALM); Test specifications for Access Technology Support (ISO 21218); Part 1: Implementation Conformance Statement (ICS) proforma	published	Revise TS in order to align with revised version of base standard	
388.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 102 760-2 V1.2.1 (2014-06) Intelligent Transport Systems (ITS); Communications Access for Land Mobiles (CALM); Test specifications for Access Technology Support (ISO 21218); Part 2: Test Suite Structure and Test Purposes (TSS & TP)	published	Revise TS in order to align with revised version of base standard	
389.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 102 760-3 V1.1.1 (2014-06) Intelligent Transport Systems (ITS); Communications Access for Land Mobiles (CALM); Test specifications for Access Technology Support (ISO 21218); Part 3: Abstract Test Suite (ATS) and partial PIXIT proforma	published	Develop TTCN-3 abstract test suite for conformance testing of IS 21218	
390.	ETSI TC ITS Intelligent Transport Systems	ETSI TR 101 611 V1.1.1 (2014-06) Intelligent Transport Systems (ITS); Testing; Conformance test specification for CALM Fast Services; FNTP/FSAP/IICP validation report	published	The ETSI Technical Report (TR) will provide the statistics of executed and validated tests which the prototype test system run against real implementations. Furthermore, it will provide a section on the validation of the test specifications and base specifications.	

	Standardization Body	Title	Status	Summary	CitySCAPE Action
391.	ETSI TC ITS Intelligent Transport Systems	ETSI TR 103 101 V1.1.1 (2014-06) Intelligent Transport Systems (ITS); Test suite validation; Access technology support ISO 21218	published	The ETSI Technical Report (TR) will provide the statistics of executed and validated tests which the prototype test system run against real implementations. Furthermore, it will provide a section on the validation of the test specifications and base specifications.	
392.	ETSI TC ITS Intelligent Transport Systems	Intelligent Transport Systems (ITS); Communications Access for Land Mobiles (CALM); Test specifications for ITS station management (ISO 24102); Part 1: Protocol Implementation Conformance Statement (PICS) specification	published	Maintenance - update based on change requests from STF455 and ISO TC204 WG16	
393.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 102 797-2 V1.2.1 (2014-06) Intelligent Transport Systems (ITS); Communications Access for Land Mobiles (CALM); Test specifications for ITS station management (ISO 24102); Part 2: Test Suite Structure and Test Purposes (TSS & TP)	published	Maintenance - Update TSS&TP based on change requests from STF455 / ISO TC204 WG16	
394.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 102 797-3 V1.2.1 (2014-06) Intelligent Transport Systems (ITS); Communications Access for Land Mobiles (CALM); Test specifications for ITS station management (ISO 24102); Part 3: Abstract Test Suite (ATS) and partial PIXIT proforma	published	Maintenance - Update of ATS based on change requests from STF455 and ISO TC204 WG16	

	Standardization Body	Title	Status	Summary	CitySCAPE Action
395.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 102 985-1 V1.2.1 (2014-06) Intelligent Transport Systems (ITS); Communications Access for Land Mobiles (CALM); Test specifications for non-IP networking (ISO 29281); Part 1: Protocol Implementation Conformance Statement (PICS) proforma	published	Maintenance - Update of PICS based on change requests from STF 455 and ISO TC204 WG16	
396.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 102 985-2 V1.2.1 (2014-06) Intelligent Transport Systems (ITS); Communications Access for Land Mobiles (CALM); Test specifications for non-IP networking (ISO 29281); Part 2: Test Suite Structure and Test Purposes (TSS & TP)	published	Maintenance - update of TSS&TP based on change requests from STF455 and ISO TC204 WG16	
397.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 102 985-3 V1.2.1 (2014-06) Intelligent Transport Systems (ITS); Communications Access for Land Mobiles (CALM); Test specifications for non-IP networking (ISO 29281); Part 3: Abstract Test Suite (ATS) and partial PIXIT proforma	published	Maintenance - update based on change requests from STF455 and ISO TC204 WG16	
398.	ETSI TC ITS Intelligent Transport Systems	ETSI EN 302 636-6-1 V1.2.1 (2014-05) Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 6: Internet Integration; Sub-part 1: Transmission of IPv6 Packets over GeoNetworking Protocols	published	Revision of the TS 102 636 - 6 - 1 according to ETSI TC ITS work progress; harmonization as far as possible with other standardization work and received change requests before proposing it as an EN in conformity with M/453 mandate.	

	Standardization Body	Title	Status	Summary	CitySCAPE Action
399.	ETSI TC ITS Intelligent Transport Systems	ETSI TR 103 099 V1.2.1 (2014-05) Intelligent Transport Systems (ITS); Architecture of conformance validation framework	published	The WI describes the architecture of the conformance validation framework, including test environment, codec and test adapter	
400.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 102 869-1 V1.3.1 (2014-05) Intelligent Transport Systems (ITS); Testing; Conformance test specifications for Decentralized Environmental Notification Messages (DENM); Part 1: Test requirements and Protocol Implementation Conformance Statement (PICS) proforma	published	Maintenance of the DENM Test requirements and Protocol Implementation Conformance Statement (PICS) proforma to synchronize content with EN 302 637-3 V1.2.0.	
401.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 102 869-2 V1.3.1 (2014-05) Intelligent Transport Systems (ITS); Testing; Conformance test specifications for Decentralized Environmental Notification Messages (DENM); Part 2: Test Suite Structure and Test Purposes (TSS & TP)	published	Maintenance of the DENM Test Suite Structure and Test Purposes (TSS&TP) to synchronize content with EN 302 637-3 V1.2.0.	
402.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 102 869-3 V1.3.1 (2014-05) Intelligent Transport Systems (ITS); Testing; Conformance test specifications for Decentralized Environmental Notification Messages (DENM); Part 3: Abstract Test Suite (ATS) and Protocol Implementation eXtra Information for Testing (PIXIT)	published	Maintenance of the DENM Abstract Test Suite (ATS) and Protocol Implementation eXtra Information for Testing (PIXIT) to synchronize content with EN 302 637-3 V1.2.0.	

	Standardization Body	Title	Status	Summary	CitySCAPE Action
403.	ETSI TC ITS Intelligent Transport Systems	ETSI EN 302 636-1 V1.2.1 (2014-04) Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 1: Requirements	published	Revision of the TS 102 636 - 1 according to ETSI TC ITS work progress; harmonization as far as possible with other standardization work and received change requests before proposing it as an EN in conformity with M/453 mandate.	
404.	ETSI TC ITS Intelligent Transport Systems	ETSI TR 103 061-3 V1.2.1 (2014-04) Intelligent Transport Systems (ITS); Testing; Part 3: Conformance test specifications for Geographical addressing and forwarding for point-to-point and point-to-multipoint communications; GeoNetworking validation report	published	The ETSI Technical Report (TR) will provide the statistics of executed and validated tests which the prototype test system run against real equipment. Furthermore, it will provide a section on the validation of the test specifications and base specifications.	
405.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 102 859-2 V1.2.1 (2014-04) Intelligent Transport Systems (ITS); Testing; Conformance test specifications for Transmission of IP packets over GeoNetworking; Part 2: Test Suite Structure and Test Purposes (TSS & TP)	published	Protocol conformance testing for transmission of IP over GeoNetworking as defined in TS 102 636-6-1.	
406.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 102 859-3 V1.2.1 (2014-04) Intelligent Transport Systems (ITS); Testing; Conformance test specifications for Transmission of IP packets over GeoNetworking; Part 3: Abstract Test Suite (ATS) and Protocol Implementation eXtra Information for Testing (PIXIT)	published	Protocol conformance testing for transmission of IP packets over GeoNetworking as defined in TS 102 636-6-1.	

	Standardization Body	Title	Status	Summary	CitySCAPE Action
407.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 102 859-1 V1.2.1 (2014-04) Intelligent Transport Systems (ITS); Testing; Conformance test specifications for Transmission of IP packets over GeoNetworking; Part 1: Test requirements and Protocol Implementation Conformance Statement (PICS) proforma	published	Protocol conformance testing for Transmission of IP packets over GeoNetworking as defined in TS 102 636-6-1.	
408.	ETSI TC ITS Intelligent Transport Systems	ETSI TR 103 061-1 V1.2.1 (2014-04) Intelligent Transport Systems (ITS); Testing; Part 1: Conformance test specifications for Co-operative Awareness Messages (CAM); CAM validation report	published	Revision of TS 103 061 -1 CAM validation report based on EN 302 637 - 2, converted from TS 102 637 - 2.	
409.	ETSI TC ITS Intelligent Transport Systems	ETSI TR 103 061-2 V1.2.1 (2014-04) Intelligent Transport Systems (ITS); Testing; Part 2: Conformance test specifications for Decentralized Environmental Notification basic service Messages (DENM); DENM validation report	published	Revision of TR 103 061 DENM validation report based on EN 302 637 - 3, converted from TS 103 637-3.	

	Standardization Body	Title	Status	Summary	CitySCAPE Action
410.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 102 868-1 V1.2.1 (2014-04) Intelligent Transport Systems (ITS); Testing; Conformance test specifications for Co-operative Awareness Messages (CAM); Part 1: Test requirements and Protocol Implementation Conformance Statement (PICS) proforma	published	Maintenance of the CAM Test requirements and Protocol Implementation Conformance Statement (PICS) proforma.	
411.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 102 871-3 V1.2.1 (2014-04) Intelligent Transport Systems (ITS); Testing; Conformance test specifications for GeoNetworking ITS-G5; Part 3: Abstract Test Suite (ATS) and Protocol Implementation eXtra Information for Testing (PIXIT)	published	Protocol conformance testing for GeoNetworking/ITS-G5 as defined in TS 102 636-4-1 and TS 102 636-4-2	
412.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 102 871-1 V1.2.1 (2014-04) Intelligent Transport Systems (ITS); Testing; Conformance test specifications for GeoNetworking ITS-G5; Part 1: Test requirements and Protocol Implementation Conformance Statement (PICS) proforma	published	Protocol conformance testing for GeoNetworking/ITS-G5 as defined in TS 102 636-4-1 and TS 102 636-4-2	
413.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 102 871-2 V1.2.1 (2014-04) Intelligent Transport Systems (ITS); Testing; Conformance test specifications for GeoNetworking ITS-G5; Part 2: Test Suite Structure and Test Purposes (TSS & TP)	published	Protocol conformance testing for GeoNetworking/ITS-G5 as defined in TS 102 636-4-1 and TS 102 636-4-2	

	Standardization Body	Title	Status	Summary	CitySCAPE Action
414.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 102 868-2 V1.2.1 (2014-04) Intelligent Transport Systems (ITS); Testing; Conformance test specifications for Co-operative Awareness Messages (CAM); Part 2: Test Suite Structure and Test Purposes (TSS & TP)	published	Maintenance of CAM Test Suite Structure and Test Purposes (TSS&TP).	
415.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 102 868-3 V1.2.1 (2014-04) Intelligent Transport Systems (ITS); Testing; Conformance test specifications for Co-operative Awareness Messages (CAM); Part 3: Abstract Test Suite (ATS) and Protocol Implementation eXtra Information for Testing (PIXIT)	published	Maintenance of the CAM Abstract Test Suite (ATS) and Protocol Implementation eXtra Information for Testing (PIXIT).	
416.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 102 723-11 V1.1.1 (2013-12) Intelligent Transport Systems (ITS); OSI cross-layer topics; Part 11: Interface between networking and transport layer and facilities layer	published	Specifies Interface(s) between the ITS network&transport layer and the ITS facility layer including interface services and service primitives which are extendible in order to achieve general applicability. Specifies related procedures and common parameters. Development is with consultation of TC ITS WG1 and WG2.	
417.	ETSI TC ITS Intelligent Transport Systems	ETSI EN 302 636-2 V1.2.1 (2013-11) Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 2: Scenarios	published	Revision of the TS 102 636 - 2 according to ETSI TC ITS work progress; harmonization as far as possible with other standardization work and received change requests before proposing it as an EN in conformity with M/453 mandate.	

	Standardization Body	Title	Status	Summary	CitySCAPE Action
418.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 101 539-3 V1.1.1 (2013-11) Intelligent Transport Systems (ITS); V2X Applications; Part 3: Longitudinal Collision Risk Warning (LCRW) application requirements specification	published	Description of the Longitudinal Collision Risk Warning application and development of related specifications on the necessary parameters and conditions to operate the application using Co-operative Awareness Message (CAM) and / or of Decentralized Environmental Notification Message (DENM).	
419.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 102 636-4-2 V1.1.1 (2013-10) Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 4: Geographical addressing and forwarding for point-to-point and point-to-multipoint communications; Sub-part 2: Media-dependent functionalities for ITS-G5	published	The deliverable will specify media-dependent functionalities for GeoNetworking as a network protocol for ad hoc routing in vehicular environments, including vehicle-to-vehicle and vehicle-to-infrastructure wireless communication. More specifically, the deliverable will specify the media-dependent functionalities for 5 GHz media (5,9 GHz).	
420.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 102 894-1 V1.1.1 (2013-08) Intelligent Transport Systems (ITS); Users and applications requirements; Part 1: Facility layer structure, functional requirements and specifications	published	To define ITS station facility layer structure, identify required facilities and components for BSA development. To provide necessary specifications for facilities components.	
421.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 101 539-1 V1.1.1 (2013-08) Intelligent Transport Systems (ITS); Users and applications requirements; Part 1: Facility layer structure, functional requirements and specifications	published	Description of the Co-operative Awareness application and development of related specifications on the necessary parameters and conditions to operate the application using Co-operative Awareness Message (CAM) and / or of Decentralized Environmental Notification Message (DENM).	

	Standardization Body	Title	Status	Summary	CitySCAPE Action
422.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 102 869-2 V1.2.1 (2013-08) Intelligent Transport Systems (ITS); Users and applications requirements; Part 1: Facility layer structure, functional requirements and specifications	published	Maintenance of the DNM Test Suite Structure and Test Purposes (TSS&TP).	
423.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 102 869-3 V1.2.1 (2013-08) Intelligent Transport Systems (ITS); Testing; Conformance test specification for Decentralized Environmental Notification Messages (DENM); Part 3: Abstract Test Suite (ATS) and Protocol Implementation eXtra Information for Testing (PIXIT)	published	Maintenance of the DENM Abstract Test Suite (ATS) and Protocol Implementation eXtra Information for Testing (PIXIT).	
424.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 102 894-2 V1.1.1 (2013-08) Intelligent Transport Systems (ITS); Users and applications requirements; Part 2: Applications and facilities layer common data dictionary	published	Definition and specifications on the common data container at the applications and facilities layer. The common data container includes the definition, syntax and semantic specifications of all the data elements/data frames used in the applications and facilities layer messages.	

	Standardization Body	Title	Status	Summary	CitySCAPE Action
425.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 102 869-1 V1.2.1 (2013-08) Intelligent Transport Systems (ITS); Testing; Conformance test specification for Decentralized Environmental Notification Messages (DENM); Part 1: Test requirements and Protocol Implementation Conformance Statement (PICS) proforma	published	Maintenance of the DENM Test requirements and Protocol Implementation Conformance Statement (PICS) proforma.	
426.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 103 096-1 V1.1.1 (2013-07) Intelligent Transport Systems (ITS); Testing; Conformance test specification for TS 102 867 and TS 102 941; Part 1: Protocol Implementation Conformance Statement (PICS)	published	Provides the PICS as pre-requisite for tests of ITS use of IEEE 1609.2 messages and data structures defined in TS 102 867 and TS 102 941	
427.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 103 096-2 V1.1.1 (2013-07) Intelligent Transport Systems (ITS); Testing; Conformance test specification for TS 102 867 and TS 102 941; Part 2: Test Suite Structure and Test Purposes (TSS&TP)	published	Provide the Test Suite Structure and Test Plans to be used to test the ITS use of IEEE 1609.2 messages and data structures defined in TS 102 867 and TS 102 941	
428.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 103 096-3 V1.1.1 (2013-07) Intelligent Transport Systems (ITS); Testing; Conformance test specification for TS 102 867 and TS 102 941; Part 3: Abstract Test Suite (ATS) and Protocol Implementation eXtra Information for Testing (PIXIT)	published	To develop test cases from the TSS&TP for TS 102 867 and TS 102 941 for the purposes of conformance testing of ITS Security as defined in those documents which themselves use capabilities defined in IEEE 1609.2. The test cases to be made available in TTCN3.	

	Standardization Body	Title	Status	Summary	CitySCAPE Action
429.	ETSI TC ITS Intelligent Transport Systems	ETSI EN 302 663 V1.2.1 (2013-07) Intelligent Transport Systems (ITS); Access layer specification for Intelligent Transport Systems operating in the 5 GHz frequency band	published	Revision making of ES 202 663 to upgrade to EN, Take into account 802.11p final changes and 802.11p transfer to 802.11, Linkage to TS 102 792 needs to be clarified, other changes based on new information from G5 related projects	
430.	ETSI TC ITS Intelligent Transport Systems	ETSI ES 200 674-1 V2.4.1 (2013-05) Intelligent Transport Systems (ITS); Road Transport and Traffic Telematics (RTTT); Dedicated Short Range Communications (DSRC); Part 1: Technical characteristics and test methods for High Data Rate (HDR) data transmission equipment operating in the 5,8 GHz Industrial, Scientific and Medical (ISM) band	published	Correct minor editorial and technical inconsistencies found in the standard after STF 422 test specifications.	
431.	ETSI TC ITS Intelligent Transport Systems	ETSI TR 101 607 V1.1.1 (2013-05) Intelligent Transport Systems (ITS); Cooperative ITS (C-ITS); Release 1	published	To develop a TC ITS Release process and identify the ETSI deliverables that form Release 1 for Cooperative ITS.	
432.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 103 097 V1.1.1 (2013-04) Intelligent Transport Systems (ITS); Security; Security header and certificate formats	published	Provide an extended security protocol header format including a certificate format as an adaption of IEEE 1609.2 for the purpose of ITS G5 messages	

	Standardization Body	Title	Status	Summary	CitySCAPE Action
433.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 102 708-2-1 V1.3.1 (2013-03) Intelligent Transport Systems (ITS); RTTT; Test specifications for High Data Rate (HDR) data transmission equipment operating in the 5,8 GHz ISM band; Part 2: Application Layer; Sub-part 1: Protocol Implementation Conformance Statement (PICS) proforma specification	published	Correct minor editorial and technical inconsistencies	
434.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 102 708-2-2 V1.4.1 (2013-03) Intelligent Transport Systems (ITS); RTTT; Test specifications for High Data Rate (HDR) data transmission equipment operating in the 5,8 GHz ISM band; Part 2: Application Layer; Sub-Part 2: Test Suite Structure and Test Purposes (TSS&TP)	published	Correct minor editorial and technical inconsistencies	
435.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 102 708-2-3 V1.4.1 (2013-03) Intelligent Transport Systems (ITS); RTTT; Test specifications for High Data Rate (HDR) data transmission equipment operating in the 5,8 GHz ISM band; Part 2: Application Layer; Sub-part 3: Abstract Test Suite (ATS) and partial PIXIT proforma	published	Correct minor editorial and technical inconsistencies. Implement additional tests as required by a certification authority.	

	Standardization Body	Title	Status	Summary	CitySCAPE Action
436.	ETSI TC ITS Intelligent Transport Systems	ETSI TR 102 965 V1.1.1 (2013-03) Intelligent Transport Systems (ITS); Application Object Identifier (ITS-AID); Registration list	published	Create and maintain a list of ITS-AID values for purposes of ETSI TC ITS. Harmonize assignments with other SDOs maintaining similar lists. The list presented in the TR shall show the global situation, i.e. including the entries of other SDOs. Details on a future registration authority and registration records used there are outside the scope of this TR.	
437.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 102 917-1 V1.1.1 (2013-01) Intelligent Transport Systems (ITS); Test specifications for the channel congestion control algorithms operating in the 5,9 GHz range; Part 1: Protocol Implementation Conformance Statement (PICS)	published	Test specifications for the channel congestion control algorithms operating in the 5,9 GHz range; Part 1: RF conformance and Protocol Implementation Conformance Statement (PICS) proforma	
438.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 102 917-2 V1.1.1 (2013-01) Intelligent Transport Systems (ITS); Test specifications for the channel congestion control algorithms operating in the 5,9 GHz range; Part 2: Test Suite Structure and Test Purposes (TSS & TP)	published	Test specifications for the channel congestion control algorithms operating in the 5,9 GHz range; Test Suite Structure and Test Purposes (TSS & TP)	
439.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 102 917-3 V1.1.1 (2013-01) Intelligent Transport Systems (ITS); Test specifications for the channel congestion control algorithms operating in the 5,9 GHz range; Part 3: Abstract Test Suite (ATS) and partial Protocol Implementation eXtra Information for Testing (PIXIT)	published	Test specifications for the channel congestion control algorithms operating in the 5,9 GHz range.; Abstract Test Suite (ATS) and Protocol Implementation eXtra Information for Testing (PIXIT)	

	Standardization Body	Title	Status	Summary	CitySCAPE Action
440.	ETSI TC ITS Intelligent Transport Systems	ETSI TR 102 960 V1.1.1 (2012-11) Intelligent Transport Systems (ITS); Test specifications for the channel congestion control algorithms operating in the 5,9 GHz range; Part 3: Abstract Test Suite (ATS) and partial Protocol Implementation eXtra Information for Testing (PIXIT)	published	Without the use of special mitigation techniques, European CEN Dedicated Short Range Communication (DSRC) equipment operating in the frequency range from 5 795 MHz to 5 815 MHz might suffer from harmful interference caused by Intelligent Transport Systems (ITS) using adjacent frequency bands. The produced Technical Report (TR) will evaluate the detailed need of mitigation techniques and the corresponding parameters to avoid this interference. The evaluation will be based on simulation and measurements.	
441.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 102 723-10 V1.1.1 (2012-11) Intelligent Transport Systems (ITS); OSI cross-layer topics; Part 10: Interface between access layer and networking & transport layer	published	Specification of the interface(s) between Access Layer and Network & Transport Layer. It includes specification, e.g SAP services and service primitives which are extendible in order to achieve general applicability and related procedures as well as Link Layer Control.	
442.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 102 723-1 V1.1.1 (2012-11) Intelligent Transport Systems (ITS); OSI cross-layer topics; Part 1: Architecture and addressing schemes	published	Specifies the architectural approach to interconnect the various layers and entities of the ITS station reference architecture. Specifies a unique addressing scheme for communication interfaces. Specifies station-local management communications. Specifies common terms and definitions.	
443.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 102 723-2 V1.1.1 (2012-11) Intelligent Transport Systems (ITS); OSI cross-layer topics; Part 2: Management information base	published	Specifies the general approach for a management information base built with the latest version of ASN.1 and being compliant with the MIB approach of IEEE 802.11. Specifies common parameters. Specifies the minimum MIB for common parameters. Investigates the possibility to alternatively also use XML in addition to ASN.1. If feasible, appropriate requirements are specified.	
444.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 102 723-3 V1.1.1 (2012-11) Intelligent Transport Systems (ITS); OSI cross-layer topics; Part 3: Interface between management entity and access layer	published	Specifies Interface(s) between the ITS management entity and the ITS access layer including interface services and service primitives which are extendible in order to achieve general applicability. Specifies related procedures and common parameters. Development is with consultation of TC ITS WG4.	

	Standardization Body	Title	Status	Summary	CitySCAPE Action
445.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 102 723-4 V1.1.1 (2012-11) Intelligent Transport Systems (ITS); OSI cross-layer topics; Part 4: Interface between management entity and networking & transport layer	published	Specifies Interface(s) between the ITS management entity and the ITS network&transport layer including interface services and service primitives which are extendible in order to achieve general applicability. Specifies related procedures and common parameters. Development is with consultation of TC ITS WG3.	
446.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 102 723-5 V1.1.1 (2012-11) Intelligent Transport Systems (ITS); OSI cross-layer topics; Part 5: Interface between management entity and facilities layer	published	Specifies Interface(s) between the ITS management entity and the ITS facilities layer including interface services and service primitives which are extendible in order to achieve general applicability. Specifies related procedures and common parameters. Development is with consultation of TC ITS WG1.	
447.	ETSI TC ITS Intelligent Transport Systems	ETSI TR 103 061-5 V1.1.1 (2012-11) Intelligent Transport Systems (ITS); Testing; Part 5: IPv6 over GeoNetworking validation report	published	The ETSI Technical Report (TR) will provide the statistics of executed and validated tests which the prototype test system run against real equipment. Furthermore, it will provide a section on the validation of the test specifications and base specifications.	
448.	ETSI TC ITS Intelligent Transport Systems	ETSI TR 103 061-4 V1.1.1 (2012-11) Intelligent Transport Systems (ITS); Testing; Part 4: Conformance test specification for GeoNetworking Basic Transport Protocol (BTP); GeoNetworking BTP validation report	published	The ETSI Technical Report (TR) will provide the statistics of executed and validated tests which the prototype test system run against real equipment. Furthermore, it will provide a section on the validation of the test specifications and base specifications.	
449.	ETSI TC ITS Intelligent Transport Systems	ETSI TR 103 061-3 V1.1.1 (2012-11) Intelligent Transport Systems (ITS); Testing; Part 3: Conformance test specification for Geographical addressing and forwarding for point-to-point and point-to-multipoint communications; GeoNetworking validation report	published	The ETSI Technical Report (TR) will provide the statistics of executed and validated tests which the prototype test system run against real equipment. Furthermore, it will provide a section on the validation of the test specifications and base specifications.	

	Standardization Body	Title	Status	Summary	CitySCAPE Action
450.	ETSI TC ITS Intelligent Transport Systems	ETSI TR 103 061-1 V1.1.1 (2012-11) Intelligent Transport Systems (ITS); Testing; Part 1: Conformance test specification for Co-operative Awareness Messages (CAM); CAM validation report	published	The ETSI Technical Report (TR) will provide the statistics of executed and validated tests which the prototype test system run against real equipment. Furthermore, it will provide a section on the validation of the test specifications and base specifications.	
451.	ETSI TC ITS Intelligent Transport Systems	ETSI TR 103 061-2 V1.1.1 (2012-11) Intelligent Transport Systems (ITS); Testing; Part 2: Conformance test specification for Decentralized Environmental Notification basic Service Message (DENM); DENM validation report	published	The ETSI Technical Report (TR) will provide the statistics of executed and validated tests which the prototype test system run against real equipment. Furthermore, it will provide a section on the validation of the test specifications and base specifications.	
452.	ETSI TC ITS Intelligent Transport Systems	ETSI TR 103 099 V1.1.1 (2012-11) Intelligent Transport Systems (ITS); Architecture of conformance validation framework	published	The WI describes the architecture of the conformance validation framework, including test environment, codec and test adapter.	
453.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 102 724 V1.1.1 (2012-10) Intelligent Transport Systems (ITS); Harmonized Channel Specifications for Intelligent Transport Systems operating in the 5 GHz frequency band	published	The specifications for operation in the 5 GHz range to satisfy the harmonised usage of the designated spectrum by control and service channels including usage of channels for road- safety related ITS applications. This will also include transmit and receive restrictions (likely to have implications on TPC). Reference usage scenarios and parameters will be depicted in informative annexes that justify the specifications. Co-channel and adjacent channel interference considerations will be encompassed.	

	Standardization Body	Title	Status	Summary	CitySCAPE Action
454.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 102 792 V1.1.1 (2012-10) Intelligent Transport Systems (ITS); Mitigation techniques to avoid interference between European CEN Dedicated Short Range Communication (CEN DSRC) equipment and Intelligent Transport Systems (ITS) operating in the 5 GHz frequency range	published	Without the use of special mitigation techniques, European CEN Dedicated Short Range Communication (DSRC) equipment operating in the frequency range from 5 795 MHz to 5 815 MHz can suffer from harmful interference caused by Intelligent Transport Systems (ITS) using adjacent frequency bands. The produced document will specify procedures on how to avoid this interference.	
455.	ETSI TC ITS Intelligent Transport Systems	ETSI ES 200 674-1 V2.3.1 (2012-08) Intelligent Transport Systems (ITS); Road Transport and Traffic Telematics (RTTT); Dedicated Short Range Communications (DSRC); Part 1: Technical characteristics and test methods for High Data Rate (HDR) data transmission equipment operating in the 5,8 GHz Industrial, Scientific and Medical (ISM) band	published	Correct minor editorial and technical inconsistencies found in the standard after STF 422 test specifications.	
456.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 102 797-2 V1.1.1 (2012-08) Intelligent Transport Systems (ITS); Communications Access for Land Mobiles (CALM); Test specifications for ITS station management (ISO 24102); Part 2: Test Suite Structure and Test Purposes (TSS&TP)	published	Protocol conformance testing for the air interface manager that is part of the CALM management and that serves CALM communication interfaces via the M-SAP as outlined in ISO 24102.	

	Standardization Body	Title	Status	Summary	CitySCAPE Action
457.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 102 797-1 V1.1.1 (2012-08) Intelligent Transport Systems (ITS); Communications Access for Land Mobiles (CALM); Test specifications for ITS station management (ISO 24102); Part 1: Protocol Implementation Conformance Statement (PICS) specification	published	Protocol conformance testing for the air interface manager that is part of the CALM management and that serves CALM communication interfaces via the M-SAP as outlined in ISO 24102.	
458.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 102 797-3 V1.1.1 (2012-08) Intelligent Transport Systems (ITS); Communications Access for Land Mobiles (CALM); Test specifications for ITS station management (ISO 24102); Part 3: Abstract Test Suite (ATS) and partial PIXIT proforma	published	Development of abstract test suite (TTCN-3) and partial PIXIT proforma for ISO 24102	
459.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 102 985-1 V1.1.1 (2012-07) Intelligent Transport Systems (ITS); Communications Access for Land Mobiles (CALM); Test specifications for non-IP networking (ISO 29281); Part 1: Protocol Implementation Conformance Statement (PICS) proforma	published	Specifies the global framework for conformance and interoperability testing in ITS.	
460.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 102 985-2 V1.1.1 (2012-07) Intelligent Transport Systems (ITS); Communications Access for Land Mobiles (CALM); Test specifications for non-IP networking (ISO 29281); Part 2: Test Suite Structure and Test Purposes (TSS&TP)	published	Specifies the global framework for conformance and interoperability testing in ITS.	

	Standardization Body	Title	Status	Summary	CitySCAPE Action
461.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 102 985-3 V1.1.1 (2012-07) Intelligent Transport Systems (ITS); Communications Access for Land Mobiles (CALM); Test specifications for non-IP networking (ISO 29281); Part 3: Abstract Test Suite (ATS) and partial PIXIT proforma	published	Specifies the global framework for conformance and interoperability testing in ITS.	
462.	ETSI TC ITS Intelligent Transport Systems	Intelligent Transport Systems (ITS); Infrastructure to Vehicle Communication; Electric Vehicle Charging Spot Notification Specification	published	Development of a Technical Specification for the broadcasting of dynamic information from a roadside unit / charging spot to Electric Vehicles (EV) related to the availability and capabilities of local EV Charging Spot(s).	
463.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 102 940 V1.1.1 (2012-06) Intelligent Transport Systems (ITS); Security; ITS communications security architecture and security management	published	This technical specification shall include security services specification, certificate and pseudonyms management, definition of Security Infrastructure/PKI processes and interfaces as well as basic policies and guidelines for trust establishment (e.g. Certificate authorities organisation and cross-certification), further requirements if identified.	
464.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 102 941 V1.1.1 (2012-06) Intelligent Transport Systems (ITS); Security; Trust and Privacy Management	published	This technical specification shall include specification for identity and key management functions, e.g. for issuing and managing long-term and short-term identities.	
465.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 102 942 V1.1.1 (2012-06) Intelligent Transport Systems (ITS); Security; Access Control	published	This technical specification shall include specification of authentication/authorization services to avoid unauthorized access and specification of measures to ensure the required level of security and privacy for message communication.	
466.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 102 943 V1.1.1 (2012-06) Intelligent Transport Systems (ITS); Security; Confidentiality services	published	This technical specification shall include specification of measures to ensure the required level of confidentiality of information for participants in the co-operative ITS.	

	Standardization Body	Title	Status	Summary	CitySCAPE Action
467.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 102 708-2-2 V1.3.1 (2012-06) Intelligent Transport Systems (ITS); RTTT; Test specifications for High Data Rate (HDR) data transmission equipment operating in the 5,8 GHz ISM band; Part 2: Application Layer; Sub-Part 2: Test Suite Structure and Test Purposes (TSS&TP)	published	Revise TSS&TP to reflect additional test requirements due to the revision of ES 200 674-1.	
468.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 102 708-2-3 V1.3.1 (2012-06) Intelligent Transport Systems (ITS); RTTT; Test specifications for High Data Rate (HDR) data transmission equipment operating in the 5,8 GHz ISM band; Part 2: Application Layer; Sub-Part 3: Abstract Test Suite (ATS) and partial PIXIT proforma	published	Revise ATS to reflect additional test requirements due to the revision of ES 200 67.	
469.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 102 916-1 V1.1.1 (2012-05) Intelligent Transport Systems (ITS); Test specifications for the methods to ensure coexistence of Cooperative ITS G5 with RTTT DSRC; Part 1: Protocol Implementation Conformance Statement (PICS)	published	Test specifications for the methods to ensure coexistence of cooperative ITS G5 with RTTT DSRC; Part 1: RF conformance and Protocol Implementation Conformance Statement (PICS) proforma	

	Standardization Body	Title	Status	Summary	CitySCAPE Action
470.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 102 916-2 V1.1.1 (2012-05) Intelligent Transport Systems (ITS); Test specifications for the methods to ensure coexistence of Cooperative ITS G5 with RTTT DSRC; Part 2: Test Suite Structure and Test Purposes (TSS&TP)	published	Test specifications for the methods to ensure coexistence of cooperative ITS G5 with RTTT DSRC; Test Suite Structure and Test Purposes (TSS & TP)	
471.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 102 916-3 V1.1.1 (2012-05) Intelligent Transport Systems (ITS); Test specifications for the methods to ensure coexistence of Cooperative ITS G5 with RTTT DSRC; Part 3: Abstract Test Suite (ATS) and partial Protocol Implementation eXtra Information for Testing (PIXIT)	published	Test specifications for the methods to ensure coexistence of cooperative ITS G5 with RTTT DSRC; Abstract Test Suite (ATS) and Protocol Implementation eXtra Information for Testing (PIXIT)	
472.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 102 708-2-3 V1.2.1 (2012-03) Intelligent Transport Systems (ITS); RTTT; Test specifications for High Data Rate (HDR) data transmission equipment operating in the 5,8 GHz ISM band; Part 2: Application Layer; Sub-Part 3: Abstract Test Suite (ATS) and partial PIXIT proforma	published	Revise ATS to reflect additional test requirements due to the revision of ES 200 67.	

	Standardization Body	Title	Status	Summary	CitySCAPE Action
473.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 102 708-2-2 V1.2.1 (2012-02) Intelligent Transport Systems (ITS); RTTT; Test specifications for High Data Rate (HDR) data transmission equipment operating in the 5,8 GHz ISM band; Part 2: Application Layer; Sub-Part 2: Test Suite Structure and Test Purposes (TSS&TP)	published	Revise TSS&TP to reflect additional test requirements due to the revision of ES 200 674	
474.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 102 708-2-1 V1.2.1 (2012-02) Intelligent Transport Systems (ITS); RTTT; Test specifications for High Data Rate (HDR) data transmission equipment operating in the 5,8 GHz ISM band; Part 2: Application Layer; Sub-Part 1: Protocol Implementation Conformance Statement (PICS) proforma specification	published	Revise Protocol Implementation Conformance Statement to reflect additional test requirements due to the revision of ES 200 674	

	Standardization Body	Title	Status	Summary	CitySCAPE Action
475.	ETSI TC ITS Intelligent Transport Systems	ETSI TR 102 962 V1.1.1 (2012-02) Intelligent Transport Systems (ITS); Framework for Public Mobile Networks in Cooperative ITS (C-ITS)	published	<p>The scope of the work item is to</p> <ul style="list-style-type: none"> - analyse cooperative ITS services using public mobile cellular networks for communications between ITS stations in order to identify related functional requirements on the ITS architecture, - identify required amendments / modifications of existing standards on cooperative ITS in order to enable usage of public mobile cellular networks, - identify functionality to be specified in new ITS standards to be developed under M/453. The result is to be presented as an ETSI Technical Report. <p>Starting from the architecture described in the published standard ITS Communication Architecture EN 302 665 v1.1.1, and considering primarily the Basic Set of Applications defined in ETSI TR 102 638, a critical assessment of the applicability of the 3G and 4G mobile network access to support the described application scenarios will be provided.</p> <p>This analysis aims to refer to technical standards developed by 3GPP and ETSI TC M2M as much as possible.</p> <p>This analysis is based on the ITS station architecture and also covers security aspects.</p> <p>Additional technical background provided by R&D projects such as CoCAR (http://www.aktiv-online.org/english/aktiv-cocar.html), CoCARx (the follow-on project including integration between LTE and DSRC access technologies), and CVIS (http://www.cvisproject.org/) is intended to be considered for the development of the Technical Report.</p> <p>Related standards from other SDOs working on cooperative ITS also will be considered as appropriate.</p> <p>This approach is coherent with the spirit of the "Joint CEN and ETSI Response to Mandate M/453", with specific reference to clause 3.3. Standardisation for Co-operative systems covering other media and clause 4.2.3. National R&D projects including national FOTs.</p>	
476.	ETSI TC ITS Intelligent Transport Systems	ETSI TR 102 861 V1.1.1 (2012-01) Intelligent Transport Systems (ITS); STDMA recommended parameters and settings for cooperative ITS; Access Layer Part	published	An ETSI TR on the recommended parameter settings for using STDMA.	

	Standardization Body	Title	Status	Summary	CitySCAPE Action
477.	ETSI TC ITS Intelligent Transport Systems	ETSI TR 102 862 V1.1.1 (2011-12) Intelligent Transport Systems (ITS); Performance Evaluation of Self-Organizing TDMA as Medium Access Control Method Applied to ITS; Access Layer Part	published	An ETSI TR on the performance of STDMA in road traffic scenarios.	
478.	ETSI TC ITS Intelligent Transport Systems	ETSI EN 302 931 V1.1.1 (2011-07) Intelligent Transport Systems (ITS); Vehicular Communications; Geographical Area Definition	published	Specifies types and definition of geographical areas based on basic geometric shapes. Defines the geographical destination area for the GeoNetworking protocol headers. Defines basic geometric operations to determine whether a point is located inside, outside or at the border of a geometric shape. Out of scope are existing location referencing schemes and definition of SAPs. Out of scope is encoding of the definitions in the protocols.	
479.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 102 687 V1.1.1 (2011-07) Intelligent Transport Systems (ITS); Vehicular Communications; Geographical Area Definition	published	TPC specifications for operation in the 5 GHz range to satisfy: regulatory requirement, congestion control and networking, inter-layer management, further requirements if identified.	
480.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 102 636-4-1 V1.1.1 (2011-06) Intelligent Transport System (ITS); Vehicular communications; GeoNetworking; Part 4: Geographical addressing and forwarding for point-to-point and point-to-multipoint communications; Sub-part 1: Media-Independent Functionality	published	The deliverable will specify a network protocol for ad hoc routing in vehicular environments, including vehicle-to-vehicle and vehicle-to-infrastructure wireless communication. The protocol will support communication based on concepts for geographical addressing and forwarding (Geocast). It provides mechanisms for periodic messaging and multi-hop, robust, efficient, reliable, secure and anonymous communication.	

	Standardization Body	Title	Status	Summary	CitySCAPE Action
481.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 102 871-3 V1.1.1 (2011-06) Intelligent Transport Systems (ITS); Testing; Conformance test specifications for GeoNetworking ITS-G5; Part 3: Abstract Test Suite (ATS) and Protocol Implementation eXtra Information for Testing (PIXIT)	published	Protocol conformance testing for GeoNetworking/ITS-G5 as defined in TS 102 636-4-1 and TS 102 636-4-2	
482.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 102 871-1 V1.1.1 (2011-06) Intelligent Transport Systems (ITS); Testing; Conformance test specifications for GeoNetworking ITS-G5; Part 1: Test requirements and Protocol Implementation Conformance Statement (PICS) proforma	published	Protocol conformance testing for GeoNetworking/ITS-G5 as defined in TS 102 636-4-1 and TS 102 636-4-2	
483.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 102 871-2 V1.1.1 (2011-06) Intelligent Transport Systems (ITS); Testing; Conformance test specifications for GeoNetworking ITS-G5; Part 2: Test Suite Structure and Test Purposes (TSS&TP)	published	Protocol conformance testing for GeoNetworking/ITS-G5 as defined in TS 102 636-4-1 and TS 102 636-4-2	
484.	ETSI TC ITS Intelligent Transport Systems	ETSI TR 102 863 V1.1.1 (2011-06) Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Local Dynamic Map (LDM); Rationale for and guidance on standardization	published	Provide guidance on Local Dynamic Map (LDM) standardization after analyzing the needs for communications standards related to the LDM to be developed.	

	Standardization Body	Title	Status	Summary	CitySCAPE Action
485.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 102 860 V1.1.1 (2011-05) Intelligent Transport Systems (ITS); Classification and management of ITS application objects	published	Specifies classes of ITS applications. Specifies the procedural framework of managing ITS applications in the context of the ITS station reference architecture including procedures for registration. Specifies a globally unique ITS application ID for global applicability based on the developments at CEN TC278 WG12 and WG16 and ISO TC204 WG16 and WG18, and considering the development at IEEE WAVE. Specifying an ASN.1 module providing the format of the ITS application ID.	
486.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 102 869-3 V1.1.1 (2011-03) Intelligent Transport Systems (ITS); Testing; Conformance test specification for Decentralized Environmental Notification Messages (DENM); Part 3: Abstract Test Suite (ATS) and Protocol Implementation eXtra Information for Testing (PIXIT)	published	Monitor, support and report to WG1 on the work achieved by the related STF for the development of the DNM Abstract Test Suite (ATS) and Protocol Implementation eXtra Information for Testing (PIXIT).	
487.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 102 869-1 V1.1.1 (2011-03) Intelligent Transport Systems (ITS); Testing; Conformance test specification for Decentralized Environmental Notification Messages (DENM); Part 1: Test requirements and Protocol Implementation Conformance Statement (PICS) proforma	published	Monitor, support and report to WG1 on the work achieved by the related STF for the development of the DNM Test requirements and Protocol Implementation Conformance Statement (PICS) proforma.	

	Standardization Body	Title	Status	Summary	CitySCAPE Action
488.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 102 869-2 V1.1.1 (2011-03) Intelligent Transport Systems (ITS); Testing; Conformance test specification for Decentralized Environmental Notification Messages (DENM); Part 2: Test Suite Structure and Test Purposes (TSS&TP)	published	Monitor, support and report to WG1 on the work achieved by the related STF for the development of the DNM Test Suite Structure and Test Purposes (TSS&TP).	
489.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 102 868-3 V1.1.1 (2011-03) Intelligent Transport Systems (ITS); Testing; Conformance test specification for Co-operative Awareness Messages (CAM); Part 3: Abstract Test Suite (ATS) and Protocol Implementation eXtra Information for Testing (PIXIT)	published	Monitor, support and report to WG1 on the work achieved by the related STF for the development of the CAM Abstract Test Suite (ATS) and Protocol Implementation eXtra Information for Testing (PIXIT).	
490.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 102 868-1 V1.1.1 (2011-03) Intelligent Transport Systems (ITS); Testing; Conformance test specification for Co-operative Awareness Messages (CAM); Part 1: Test requirements and Protocol Implementation Conformance Statement (PICS) proforma	published	Monitor, support and report to WG1 on the work achieved by the related STF for the development of the CAM Test requirements and Protocol Implementation Conformance Statement (PICS) proforma.	

	Standardization Body	Title	Status	Summary	CitySCAPE Action
491.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 102 868-2 V1.1.1 (2011-03) Intelligent Transport Systems (ITS); Testing; Conformance test specification for Co-operative Awareness Messages (CAM); Part 2: Test Suite Structure and Test Purposes (TSS&TP)	published	Monitor, support and report to WG1 on the work achieved by the related STF for the development of the CAM Test Suite Structure and Test Purposes (TSS&TP).	
492.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 102 859-3 V1.1.1 (2011-03) Intelligent Transport Systems (ITS); Testing; Conformance test specifications for Transmission of IP packets over GeoNetworking; Part 3: Abstract Test Suite (ATS) and Protocol Implementation eXtra Information for Testing (PIXIT)	published	Protocol conformance testing for transmission of IP packets over GeoNetworking as defined in TS 102 636-6-1.	
493.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 102 859-1 V1.1.1 (2011-03) Intelligent Transport Systems (ITS); Testing; Conformance test specifications for Transmission of IP packets over GeoNetworking; Part 1: Test requirements and Protocol Implementation Conformance Statement (PICS) proforma	published	Protocol conformance testing for Transmission of IP packets over GeoNetworking as defined in TS 102 636-6-1.	

	Standardization Body	Title	Status	Summary	CitySCAPE Action
494.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 102 859-2 V1.1.1 (2011-03) Intelligent Transport Systems (ITS); Testing; Conformance test specifications for Transmission of IP packets over GeoNetworking; Part 2: Test Suite Structure and Test Purposes (TSS&TP)	published	Protocol conformance testing for transmission of IP over GeoNetworking as defined in TS 102 636-6-1.	
495.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 102 636-6-1 V1.1.1 (2011-03) Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 6: Internet Integration; Sub-part 1: Transmission of IPv6 Packets over GeoNetworking Protocols	published	The deliverable will specify mechanisms to support IPv6 over GeoNetworking.	
496.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 102 637-2 V1.2.1 (2011-03) Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service	published	Revision of Cooperative awareness message ASN.1 format as proposed by STF 405 and as adopted by WG1	
497.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 102 870-3 V1.1.1 (2011-03) Intelligent Transport Systems (ITS); Testing; Conformance test specifications for Geonetworking Basic Transport Protocol (BTP); Part 3: Abstract Test Suite (ATS) and Protocol Implementation eXtra Information for Testing (PIXIT)	published	Protocol conformance testing for GeoNetworking/ITS-G5 as defined in TS 102 636-5-1.	

	Standardization Body	Title	Status	Summary	CitySCAPE Action
498.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 102 870-1 V1.1.1 (2011-03) Intelligent Transport Systems (ITS); Testing; Conformance test specifications for GeoNetworking Basic Transport Protocol (BTP); Part 1: Test requirements and Protocol Implementation Conformance Statement (PICS) proforma	published	Protocol conformance testing for the Basic Transport Protocol (BTP) as defined in TS 102 636-5-1.	
499.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 102 870-2 V1.1.1 (2011-03) Intelligent Transport Systems (ITS); Testing; Conformance test specifications for GeoNetworking Basic Transport Protocol (BTP); Part 2: Test Suite Structure and Test Purposes (TSS&TP)	published	Protocol conformance testing for the Basic Transport Protocol (BTP) as defined in TS 102 636-5-1	
500.	ETSI TC ITS Intelligent Transport Systems	ETSI ES 200 674-1 V2.2.1 (2011-02) Intelligent Transport Systems (ITS); Road Transport and Traffic Telematics (RTTT); Dedicated Short Range Communications (DSRC); Part 1: Technical characteristics and test methods for High Data Rate (HDR) data transmission equipment operating in the 5,8 GHz Industrial, Scientific and Medical (ISM) band	published	Adjust title to reflect passing of Work Item under TC ITS from TC ERM. Rectify minor errors in the test methods following validation of TSS&TP and ATS specs provided by STF 372. Specify missing Application test methods, and convert from ES to EN, in order to provide support for EETS as requested in draft EEC Decision on EETS.	

	Standardization Body	Title	Status	Summary	CitySCAPE Action
501.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 102 636-5-1 V1.1 (2011-02) Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 5: Transport Protocols; Sub-part 1: Basic Transport Protocol	published	The deliverable will specify a transport layer protocol for wireless communication in ITS environments.	
502.	ETSI TC ITS Intelligent Transport Systems	ETSI EG 202 798 V1.1.1 (2011-01) Intelligent Transport Systems (ITS); Testing; Framework for conformance and interoperability testing	published	Specifies the global framework for conformance and interoperability testing in ITS.	
503.	ETSI TC ITS Intelligent Transport Systems	ETSI EN 302 665 V1.1.1 (2010-09) Intelligent Transport Systems (ITS); Communications Architecture	published	Definition of ITS Communications Architecture for Europe including the following views: <ul style="list-style-type: none"> - Scenario description; - Functional View and Information View; - OSI reference model view including Application View, Security View, Network&Transport View, Interface View, Management view; - Engineering view to support Implementation Guidelines for Interoperability; - Enterprise/Organizational/Operational view. 	
504.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 102 731 V1.1.1 (2010-09) Intelligent Transport Systems (ITS); Security; Security Services and Architecture	published	The document will specify mechanisms and protocols for secure and privacy-preserving communication in vehicular environments, including vehicle-to-vehicle and vehicle-to-infrastructure communication. It will provide credential and identity management, privacy and anonymity, integrity protection, authentication and authorization. It will incorporate mechanisms such as addressing schemes building on pseudonymization concepts, the protocols for address update, and for exchanging, updating, and invalidating credentials to counterfeit attacks on security and reliability of communication. Further methods to prevent malicious tracking of identity and location will be provided.	

	Standardization Body	Title	Status	Summary	CitySCAPE Action
505.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 102 637-3 V1.1.1 (2010-09) Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 3: Specifications of Decentralized Environmental Notification Basic Service	published	Specification of Communication protocols, Message format, semantics and syntax as well as key interfaces for the Decentralized Environmental Notification basic service supporting the selected Basic Set of Applications.	
506.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 102 637-1 V1.1.1 (2010-09) Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 1: Functional Requirements	published	Specification of the functional requirements for the V2V/V2I-Communication Basic Set of Applications and their assigned use cases.	
507.	ETSI TC ITS Intelligent Transport Systems	ETSI TR 102 698 V1.1.2 (2010-07) Intelligent Transport Systems (ITS); Vehicular Communications; C2C-CC Demonstrator 2008; Use Cases and Technical Specifications	published	To provide a detailed description of Use Cases demonstrated during the C2C-CC Forum and Demonstrator event 2008 and to report on the deployed corresponding technical specifications of the demonstrator system covering all communications layers.	
508.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 102 637-2 V1.1.1 (2010-04) Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service	published	Specification of communication protocols, message format, semantics and syntax as well as key interfaces for the co-operative awareness basic service supporting the defined basic set of applications.	

	Standardization Body	Title	Status	Summary	CitySCAPE Action
509.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 102 708-2-1 V1.1.1 (2010-03) Intelligent Transport Systems (ITS); RTTT; Test specifications for High Data Rate (HDR) data transmission equipment operating in the 5,8 GHz ISM band; Part 2: Application Layer Common Application Service Elements; Sub-Part 1: Protocol Implementation Conformance Statement (PICS) proforma specification	published	Protocol conformance testing for Application Layer as defined in ES 200 674-1 revised under WI RES/ERM-TG37-013.	
510.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 102 708-2-2 V1.1.1 (2010-03) Intelligent Transport Systems (ITS); RTTT; Test specifications for High Data Rate (HDR) data transmission equipment operating in the 5,8 GHz ISM band; Part 2: Application Layer Common Application Service Elements; Sub-Part 2: Test Suite Structure and Test Purposes (TSS&TP)	published	Protocol conformance testing for Application Layer as defined in ES 200 674-1 revised under WI RES/ERM-TG37-013.	

	Standardization Body	Title	Status	Summary	CitySCAPE Action
511.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 102 708-2-3 V1.1.1 (2010-03) Intelligent Transport Systems (ITS); RTTT; Test specifications for High Data Rate (HDR) data transmission equipment operating in the 5,8 GHz ISM band; Part 2: Application Layer Common Application Service Elements; Sub-Part 3: Abstract Test Suite (ATS) and partial PIXIT proforma	published	Protocol conformance testing for Application Layer as defined in ES 200 674-1 revised under WI RES/ERM-TG37-013.	
512.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 102 708-1-1 V1.1.1 (2010-03) Intelligent Transport Systems (ITS); RTTT; Test specifications for High Data Rate (HDR) data transmission equipment operating in the 5,8 GHz ISM band; Part 1: Data Link Layer; Sub-Part 1: Protocol Implementation Conformance Statement (PICS) proforma specification	published	Protocol conformance testing for Data Link Layer as defined in ES 200 674-1 revised under WI RES/ERM-TG37-013.	
513.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 102 708-1-2 V1.1.1 (2010-03) Intelligent Transport Systems (ITS); RTTT; Test specifications for High Data Rate (HDR) data transmission equipment operating in the 5,8 GHz ISM band; Part 1: Data Link Layer; Sub-Part 2: Test Suite Structure and Test Purposes (TSS&TP)	published	Protocol conformance testing for Data Link Layer as defined in ES 200 674-1 revised under WI RES/ERM-TG37-013.	

	Standardization Body	Title	Status	Summary	CitySCAPE Action
514.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 102 708-1-3 V1.1.1 (2010-03) Intelligent Transport Systems (ITS); RTTT; Test specifications for High Data Rate (HDR) data transmission equipment operating in the 5,8 GHz ISM band; Part 1: Data Link Layer; Sub-Part 3: Abstract Test Suite (ATS) and partial PIXIT proforma	published	Protocol conformance testing for Data Link Layer as defined in ES 200 674-1 revised under WI RES/ERM-TG37-013.	
515.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 102 636-1 V1.1.1 (2010-03) Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 1: Requirements	published	The document will specify the requirements of network and transport layer protocols for ad hoc routing in vehicular environments based on wireless communication technology.	
516.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 102 636-2 V1.1.1 (2010-03) Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 2: Scenarios	published	The document will specify the network scenarios for vehicle-to-vehicle and vehicle-to-infrastructure communication.	
517.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 102 636-3 V1.1.1 (2010-03) Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 2: Scenarios	published	The deliverable will specify the network architecture for vehicle-to-vehicle and vehicle-to-infrastructure wireless communication.	
518.	ETSI TC ITS Intelligent Transport Systems	ETSI TR 102 893 V1.1.1 (2010-03) Intelligent Transport Systems (ITS); Security; Threat, Vulnerability and Risk Analysis (TVRA)	published	Preparation of a full TVRA (using guidelines from ISO 15408 and TS 102 165-1) for ITS covering Vehicle to vehicle, Vehicle to roadside infrastructure (network), Vehicle to roadside standalone unit and ITS integration with Internet communication scenarios. This work shall consider the existing output from ongoing studies (eSAFETY, SEVECOM and others) and also from other standards groups including IEEE 1609.2 and ISO TC204 (CALM).	

	Standardization Body	Title	Status	Summary	CitySCAPE Action
519.	ETSI TC ITS Intelligent Transport Systems	ETSI ES 202 663 V1.1.0 (2010-01) Intelligent Transport Systems (ITS); European profile standard for the physical and medium access control layer of Intelligent Transport Systems operating in the 5 GHz frequency band	published	This European profile standard will be based on IEEE 802.11 and further requirements stated in work items for the physical and MAC layer at ETSI. This profile standard will be the base standard for developing 5 GHz ITS conformance declaration and test standards.	
520.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 102 760-1 V1.1.1 (2009-11) Intelligent Transport Systems (ITS); Test specifications for Intelligent Transport Systems; Communications Access for Land Mobiles (CALM); Medium Service Access Points (ISO 21218); Part 1: Implementation Conformance Statement (ICS) proforma	published	Protocol conformance testing for the Service Access Points of a communication interface (CI) as provided by the Communication Adaptation Layer (CAL) for communication, and as provided by the CI Management Adaptation Entity (CIMAЕ) for management of the communication interface as outlined in ISO 21218.	
521.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 102 760-2 V1.1.1 (2009-11) Intelligent Transport Systems (ITS); Test specifications for Intelligent Transport Systems; Communications Access for Land Mobiles (CALM); Medium Service Access Points (ISO 21218); Part 2: Test Suite Structure and Test Purposes (TSS&TP)	published	Protocol conformance testing for the Service Access Points of a communication interface (CI) as provided by the Communication Adaptation Layer (CAL) for communication, and as provided by the CI Management Adaptation Entity (CIMAЕ) for management of the communication interface as outlined in ISO 21218.	
522.	ETSI TC ITS Intelligent Transport Systems	ETSI TR 102 638 V1.1.1 (2009-06) Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Release 2	published	Definition of a V2V/V2I-Communication Basic Set of Applications as a basis for the specification of the basic system.	

	Standardization Body	Title	Status	Summary	CitySCAPE Action
523.	ETSI TC ITS Intelligent Transport Systems	ETSI TR 102 698 V1.1.1 (2009-06) Intelligent Transport Systems (ITS); Vehicular Communications; C2C-CC Demonstrator 2008; Use Cases and Technical Specifications	published	To provide a detailed description of Use Cases demonstrated during the C2C-CC Forum and Demonstrator event 2008 and to report on the deployed corresponding technical specifications of the demonstrator system covering all communications layers.	
524.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 102 486-1-3 V1.2.2 (2009-05) Intelligent Transport Systems (ITS); Road Transport and Traffic Telematics (RTTT); Test specifications for Dedicated Short Range Communication (DSRC) transmission equipment; Part 1: DSRC data link layer: medium access and logical link control; Sub-Part 3: Abstract Test Suite (ATS) and partial PIXIT proforma	published	To rectify minor errors in the MAC_OBU test suite following validation.	
525.	ETSI TC ITS Intelligent Transport Systems	ETSI TR 102 707 V1.1.1 (2009-05) Intelligent Transport Systems (ITS); ETSI object identifier tree; ITS domain	published	Maintain structure and numbers of universal object identifiers for TC ITS	
526.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 102 486-1-2 V1.2.1 (2008-10) Intelligent Transport Systems (ITS); Road Transport and Traffic Telematics (RTTT); Test specifications for Dedicated Short Range Communication (DSRC) transmission equipment; Part 1: DSRC data link layer: medium access and logical link control; Sub-Part 2: Test Suite Structure and Test Purposes (TSS&TP)	published	Update of TS 102 486-1-2 to take into account any comments received during validation of STF 282 deliverables.	

	Standardization Body	Title	Status	Summary	CitySCAPE Action
527.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 102 486-1-3 V1.2.1 (2008-10) Intelligent Transport Systems (ITS); Road Transport and Traffic Telematics (RTTT); Test specifications for Dedicated Short Range Communication (DSRC) transmission equipment; Part 1: DSRC data link layer: medium access and logical link control; Sub-Part 3: Abstract Test Suite (ATS) and partial PIXIT proforma	published	Update of TS 102 486-1-3 to take into account any comments received during validation of STF 282 deliverables.	
528.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 102 486-2-1 V1.2.1 (2008-10) Intelligent Transport Systems (ITS); Road Transport and Traffic Telematics (RTTT); Test specifications for Dedicated Short Range Communication (DSRC) transmission equipment; Part 2: DSRC application layer; Sub-Part 1: Protocol Implementation Conformance Statement (PICS) proforma specification	published	Update of DTS/ERM-TG37-002-1 to take into account any corrections received during validation of STF 282 deliverables.	

	Standardization Body	Title	Status	Summary	CitySCAPE Action
529.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 102 486-2-2 V1.2.1 (2008-10) Intelligent Transport Systems (ITS) Road Transport and Traffic Telematics (RTTT); Test specifications for Dedicated Short Range Communication (DSRC) transmission equipment; Part 2: DSRC application layer; Sub-Part 2: Test Suite Structure and Test Purposes (TSS&TP)	published	Update of TS 102 486-2-2 to take into account any corrections received during validation of STF 282 deliverables.	
530.	ETSI TC ITS Intelligent Transport Systems	ETSI TS 102 486-2-3 V1.2.1 (2008-10) Intelligent Transport Systems (ITS); Road Transport and Traffic Telematics (RTTT); Test specifications for Dedicated Short Range Communication (DSRC) transmission equipment; Part 2: DSRC application layer; Sub-Part 3: Abstract Test Suite (ATS) and partial PIXIT proforma	published	Update of TS 102 486-2-3 to take into account any corrections received during validation of STF 282 deliverables.	

ANNEX 3: LIST OF IDENTIFIED NON-FORMAL STANDARDS

	Organization	Title	Summary	CitySCAPE Action
1.	MobilityData	The General Transit Feed Specification (GTFS)	The Specification defines a common format for public transportation schedules and associated geographic information. GTFS "feeds" let public transit agencies publish their transit data and developers write applications that consume that data in an interoperable way.	CSG: GTFS is fully integrated to T8.2 study as it is widely implemented as part transport system interfaces
2.	MobilityData	GTFS RealTime	GTFS Realtime is a feed specification that allows public transportation agencies to provide realtime updates about their fleet to application developers. It is an extension to GTFS (General Transit Feed Specification), an open data format for public transportation schedules and associated geographic information. GTFS Realtime was designed around ease of implementation, good GTFS interoperability and a focus on passenger information	<p>CSG: GTFS/RT is fully integrated to T8.2 study as it is widely implemented as part transport system interfaces.</p> <p>SIGLA: The application SIGLA Moving is modular and natively very flexible letting to adapt the services that can be delivered case to case (i.e., PTO to PTO, City to City) making possible to tailor the services provided in parallel to the actual possibilities and IT infrastructure of each PTO. It focuses on interoperability and integrability by default making possible to use the same app for multiple PTO and mobility services at the same time. This can be in practice the app can be adopted by many cities at the same time, enabling a user to travel on multiple cities (through different PTOs) without changing application or installing many on their phone. The app is natively multi-lingual and can be adopted independently to travel on different countries' PTOs' services. The solution provides the possibility of accessing info-mobility services (e.g., checking tickets validity, creating tickets, custom alerting/notifications, etc.) also for PTOs' staff dedicated to deliver those services.</p> <p>Hereafter the Non-Formal standards used for each considered PTO and for which interoperability has been tested:</p> <ul style="list-style-type: none"> • AMT (Genova, Italy): proprietary format returned by their API • TLT (Tallin, Estonia): proprietary format returned by their API • FOLI (Finland): standard GFTS • HSL (Finland): standard GFTS

	Organization	Title	Summary	CitySCAPE Action
				<ul style="list-style-type: none"> • LSL (Finland), standard GTFS • Nysse (Finland), standard GTFS • ATAC (Rome - Italy), standard GTFS • TTE (Trento - Italy), standard GTFS Gruppo SIGLA doesn't participate in the work of this standardization working table.
3.	The Alliance for Parking Data Standards (APDS)	APDS	The Standard establishes a common language for data elements and definitions in the parking, transportation, and mobility sector that helps to facilitate seamless integration, compatibility, and communication between parking entities, the automotive industry, IT developers, map and app providers, as well as other stakeholders.	
4.	MobilityData (North American Bikeshare Systems Association (NABSA))	General Bikeshare Feed Specification (GBFS)	The Specification is the open data standard for bikeshare, providing real-time information for bikeshare systems, such as number of available docks or bikes per station. It is a specification for real-time, read-only data (any data being written back into individual bikeshare systems are excluded). The data in the specification is intended for consumption by clients intending to provide real-time (or semi-real-time) transit advice.	CSG: GBFS is integrated as part of Transport standards to be studied as part of T8.2
5.	OASIS Cyber Threat Intelligence (CTI) TC	Structured Threat Information eXpression (STIX 1.4 and 2.0)	Open-source language and serialization format, used to exchange cyber threat intelligence (CTI). It enables organizations to share CTI with one another in a consistent and machine-readable manner, allowing security communities to better understand what computer-based attacks they are most likely to see and to anticipate and/or respond to those attacks faster and more effectively.	KSP: The Collaborative Threat Intelligence Platform (CTIP) defined in Task 3.3 and implemented by AIRBUS is fed by the Kaspersky Threat Data Feeds. The Kaspersky Threat Data Feeds list of Indicators of Compromise (IOCs) is available in standard formats like STIX. ACS leverage this format inside the CTIP component to store IOCs and their contextualization data into a MISP instance. Some limitations of the model have been bypassed by upgrading the model specifically.
6.	The MITRE Corporation	MITRE ATT&CK framework	Globally-accessible knowledge base of adversary tactics and techniques based on real-world observations. It is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community.	This format is not used by default inside the CTIP component, but ACS has designed a solution that is compatible with it through the integration of commonly available plugins.

	Organization	Title	Summary	CitySCAPE Action
7.	MANDIANT	Open Indicators of Compromise (OpenIOC) Framework	Standard format and terms for describing the artifacts encountered during the course of an investigation for recording, defining, and sharing information about threat.	<p>KSP: The Collaborative Threat Intelligence Platform (CTIP) defined in Task 3.3 and implemented by AIRBUS is fed by the Kaspersky Threat Data Feeds. The Kaspersky Threat Data Feeds list of Indicators of Compromise (IOCs) is available in standard formats like OpenIOC.</p> <p>This format is not used by default inside the CTIP component, but ACS has designed a solution that is compatible with it through the integration of commonly available plugins.</p>
8.	ENISA	Cyber Security and Resilience of smart cars	The objective of this study is to identify good practices that ensure the security of smart cars against cyber threats, with the particularity that smart cars' security shall also guarantee safety. The study lists the sensitive assets present in smart cars, as well as the corresponding threats, risks, mitigation factors and possible security measures to implement. To obtain this information, experts in the fields and areas related with smart cars were contacted to gather their know-how and expertise. These exchanges led to three categories of good practices: Policy and standards, Organizational measures, and Security functions.	
9.	ENISA	Securing Smart Airports	In response to the new emerging threats faced by smart airports, this report provides a guide for airport decision makers (CISOs, CIOs, IT Directors and Head of Operations) and airport information security professionals, but also relevant national authorities and agencies that are in charge of cyber-security for airports. Based on an in depth examination of existing knowledge as well as validation interviews with subject matter experts, this report highlights the key assets of smart airports. Built on this, a detailed analysis and threats mapping was conducted with a particular focus on the vulnerabilities of smart components.	

	Organization	Title	Summary	CitySCAPE Action
10.	ENISA	ENISA good practices for security of Smart Cars	This report defines good practices for security of smart cars, namely connected and (semi-) autonomous vehicles, providing added-value features in order to enhance car users' experience and improve car safety. Taking stock of all existing standardization, legislative and policy initiatives, this report aims to serve as a reference point to promote cybersecurity for smart cars (connected and automated cars) across Europe and raise awareness on relevant threats and risks with a focus on "cybersecurity for safety".	
11.	ENISA	Cyber Security and Resilience of Intelligent Public Transport. Good practices and recommendations	This study proposes a pragmatic approach that will highlight the critical assets of Intelligent Public Transport systems. It gives an overview of the existing security measures (good practices) that could be deployed to protect these critical assets and ensure security of the IPT system, based on a survey and interviews of experts from the sector, municipalities, operators, manufacturers and policy makers.	
12.	ENISA	Security Issues in Cross-border Electronic Authentication	Improving the interoperability of electronic identification and authentication systems is a European task and a task for all Member States. Considerable efforts have been made in several projects to face the challenges of pan-European interoperability of electronic authentication and to assess the feasibility of differing approaches. ENISA analysed the current situation and assessed the security risks of electronic authentication in cross-border solutions. To visualize these risks, two different projects offering cross-border authentication have been exemplarily examined and evaluated, NETC@RDS and STORK.	
13.	ENISA	Architecture model of the transport sector in Smart Cities	The main objective of this study is to model the architecture of the transport sector in SCs and to describe good cyber security practices of IPT operators. The good practices are put into a relationship with different city maturity levels. This allows representatives of operators and municipalities to quickly assess whether or not they lag behind other cities with the same maturity level in terms of cyber security and, if so, to take appropriate actions. The study is primarily focused on the provision of practical, hands-on guidance.	

	Organization	Title	Summary	CitySCAPE Action
14.	ENISA	Cybersecurity Certification: EUCC Candidate Scheme	Following the request from the European Commission in accordance with Article 48.2 of the Cybersecurity Act, ENISA has set up an Ad Hoc Working Group to support the preparation of a candidate EU cybersecurity certification scheme as a successor to the existing schemes operating under the SOG-IS MRA. This has been named EUCC scheme (Common Criteria based European candidate cybersecurity certification scheme) and it looks into the certification of ICT products cybersecurity, based on the Common Criteria, the Common Methodology for Information Technology Security Evaluation, and corresponding standards, respectively, ISO/IEC 15408 and ISO/IEC 18045.	CSG: This scheme is part of the labelling process analyse and definition
15.	Department for Transport, UK	Rail Cyber Security Guidance to Industry	This guidance document is designed to support the rail industry in reducing its vulnerability to cyberattack. It is designed to be high-level. It sets out the principles and general approach to cyber security, as good practice. It has a particular, but not exclusive, focus on protecting infrastructure and rolling-stock systems. It incorporates bespoke advice for railway-specific systems, as well as more general advice, to form a complete approach.	
16.	Syslog	RFC 3164	RFC 3164 is a IETF document. It describes how syslog messages have been seen in traditional implementations. RFC 3164 is not a standard but rather a descriptive (“informational” in IETF terms) document. An actual standard already produced by this working group is RFC 3195, which describes how syslog can be sent reliably over a TCP connection.	SIGLA: Cyber-security is a must-have nowadays to protect the delivery and the access to all info-mobility services. Within CitySCAPE, SIGLA faces this issue enforcing cyber-security thanks to the integration of Kaspersky Mobile Security SDK providing “security by design” into the actual infrastructure of SIGLA Moving application. Furthermore, SIGLA used RFC 3164 standard in communication with SIEM, relating to threats and vulnerabilities found on individual devices. Gruppo SIGLA doesn’t participate in the work of this standardization working table.

	Organization	Title	Summary	CitySCAPE Action
17.	CIS, Center for Internet Security	CIS Critical Security Controls	<p>The Center for Internet Security Critical Security Controls for Effective Cyber Defense is a publication of best practice guidelines for cybersecurity. The guidelines consist of 18 key actions organizations should implement to block or mitigate known attacks. Controls are designed so that mainly automated means can be used to implement, apply and monitor them. Security Controls provide practical, actionable advice on cybersecurity, written in language that is easily understood by IT staff.</p>	<p>STAM and ENG leverage CIS controls to build the set of countermeasures that the organization can apply to protect its information systems. CIS controls can be selected in FIMCA as possible security measures for the organization under analysis. Each CIS control has mitigation factors that counteract the threats it may face and the cost associated with implementing them. These controls are also leveraged by ED and UPRC to assess the organization's residual risk in RITA and by FIMCA to assess financial impact.</p> <p>ED leverage CIS controls to enable organisations through RITA build appropriate countermeasures that when applied can help them protect their information systems. When a countermeasure is created in RITA is being assigned, amongst others, to the relevant CIS control and the threat that is mitigates</p>